# Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest

Portland, Oregon, June through July 2020

January 6, 2021

Homeland Security

# Contents

**I. PURPOSE** ..... **4**

**II. EXECUTIVE SUMMARY** ..... **4**

**III. BACKGROUND** ..... **6**

**IV. REVIEW** ..... **8**

**V. SUMMARY OF I&A AUTHORITIES AND RESTRICTIONS** ..... **8**

**VI. FINDINGS** ..... **12**

A. THE CURRENT AND EMERGING THREATS CENTER (CETC) WAS UNPREPARED FOR THE MISSION ASSIGNED. ..... 12

*1. The Open Source Collection Operations (OSCO) Transformation* ..... *12*

a. Threat Notifications and the Move to 24/7 Shifts ..... 12

b. Uneven Growth in OSCO Created Bottlenecks in OSIR Production and Overstressed Senior Employees. ..... 14

c. CETC's Lack of a Formalized Training Program Crippled its Workforce and Engendered Poor Performance. ..... 16

d. Impact of Poor Training. ..... 20

e. The Pressure to Quickly Report All Threats Induced Improper Collection and Dissemination. ..... 22

*2. CETC Operations* ..... *24*

a. CETC leadership provided unclear direction. ..... 24

b. CETC leadership and oversight support had a dysfunctional relationship. ..... 26

c. Treatment of U.S. Person Information in OSIRs ..... 29

d. Quantitative Performance Metrics Encouraged a High Volume of OSIRs ..... 31

e. The Outdated Publication Software Could Not Accommodate the Increase in OSIRs ..... 32

f. Increased Focus on Publishing Threat OSIRs ..... 33

g. OSIR Review Process ..... 34

B. THE DEPLOYMENT OF I&A PERSONNEL TO PORTLAND WAS POORLY PLANNED AND EXECUTED ..... 35

*1. I&A's activities were impaired from the outset by its lack of a presence in Oregon prior to George Floyd's killing.* ..... *36*

*2. Brian Murphy Directs the Deployment of FOD and OSCO Personnel on July 8 despite the lack of Adequate Planning and Preparation for Deployment.* ..... *37*

*3. OSCO's Volunteers for the Portland Deployment Lacked Experience, Training, and Equipment on Open Source Collection.* ..... *40*

*4. I&A Failed to Establish and Implement a Clear Command Structure to Oversee and Support its Deployment to Portland.* ..... *44*

C. THE THREE LEAKED OSIRS, OPERATIONAL BACKGROUND REPORTS, AND DEVICE EXPLOITATION ..... 48

*1. OSIR-04001-0932-20* ..... *49*

*2. OSIR-04001-0937-20* ..... *51*

*3. OSIR-04001-0952-20* ..... *51*

*4. Conditions That Contributed to the Publication of the Three OSIRs* ..... *52*

*5. Operational Background Reports ("Baseball Cards")* ..... *54*

*6. Exploitation of Protestor Devices* ..... *60*

D. I&A WORK ENVIRONMENT ..... 61

*1. Work climate.* ..... *61*

*2. Employee Concerns About Retaliation.* ..... *64*

*3. Politicization of Intelligence Products.* ..... *64*

*4. Marginalized Oversight.* ..... *67*

*5. Employee Resilience.* ..... *67*

**VII. RECOMMENDATIONS** ..... **68**

A. TRAINING ..... 68

*1. Reexamine Training Across I&A.* ..... *68*

*2. Certified Release Authority (CRA) training.* ..... *68*

*3. Collector training.* ..... *68*
*4. Engage with the Open Source Intelligence (OSINT) field.* ..... *69*
*5. Supervisory training for new supervisors prior to their taking their position.* ..... *69*
B. PROMULGATE STANDARD OPERATING PROCEDURES (SOPS) ..... 69
C. EXPAND WORKPLACE RESILIENCY PROGRAMS ..... 70
D. CONDUCT A HOLISTIC REVIEW OF THE STRATEGIC DIRECTION OF I&A ..... 70
E. RESOLVE WHEN UNMASKING IS APPROPRIATE ..... 70
F. RESTART THE OSIR PROCESS ..... 71
*1. Collector Engagement.* ..... *71*
*2. Collection plans should exist prior to engaging collection.* ..... *71*
G. FIX THE OSIR RELEASE PROCESS ..... 71
*1. General.* ..... *71*
*2. Split the supervisory and SDO role.* ..... *71*
*3. Expand the hiring pool for supervisors.* ..... *72*
*4. Replace HOST.* ..... *72*
H. CETC REVIEW ..... 72
*1. Evaluate whether 24/7 operations are necessary for OSCO, or if maxiflex with surge support will suffice.* ..... *72*
*2. Evaluate the utility of non-FOD deployments.* ..... *72*
*3. Consider returning OSCO reporting back to functional areas rather than general threats.* ..... *72*
*4. Consider making CETC desk officers (DOs) supervisors.* ..... *73*
*5. Better integration with ILD.* ..... *73*
*6. Reconsider OSIR quotas.* ..... *73*
*7. Validate an OSIR review process.* ..... *73*
I. CETC – NOC RELATIONSHIP ..... 74
J. COHERENT DEPLOYMENT OPERATIONS REQUIRE PLANNING. ..... 74
*1. Create an off-the-shelf Incident Action Plan (IAP) that can be used as a framework for deployments, prior to crises taking place.* ..... *74*
*2. FOD should consider incorporating other I&A elements in its plans.* ..... *74*
K. OPERATIONAL BACKGROUND REPORTS (OBRS) REVIEW AND TRAINING. ..... 74
*1. OBR review.* ..... *74*
*2. Future OBR use.* ..... *75*
*3. CETC OBR SOP.* ..... *75*
L. MURPHY AT I&A. ..... 75

Office of the General Counsel
U.S. Department of Homeland Security
Washington, DC 20528

January 6, 2021

MEMORANDUM FOR: Ian J. Brekke
Senior Official Performing the Duties of the General Counsel

Joseph B. Maher
Senior Official Performing the Duties of the Under Secretary, Intelligence & Analysis

FROM: Internal Review Team

SUBJECT: Report of Internal Review

## I. PURPOSE

This review was conducted to examine DHS Intelligence & Analysis (I&A) open source collection and reporting activities related to the civil unrest in Portland, Oregon between May 24, 2020 to August 4, 2020, and to address the culture and morale of the I&A workforce.

## II. EXECUTIVE SUMMARY

At the request of the Acting Secretary of Homeland Security, through the then-Acting General Counsel, this internal review was conducted to examine facts and circumstances regarding the collection and publication of three Open Source Intelligence Reports (OSIRs) that reported on the activities of U.S. journalists who published unclassified I&A materials that were provided to them without authorization.[1] The review also examined the command and workforce environment at DHS I&A, the handling of a possible request for I&A to exploit certain devices

[1] Memorandum from Chad F. Wolf, Acting Secretary, DHS, "Discontinuation of Collection of Information Involving U.S. Members of the Press," dated July 31, 2020.

seized by the Federal Protective Services (FPS), and the potential politicization of intelligence products. [2]

While deployed to Portland, OR, in July 2020, in support of on-going law enforcement operations, members of the DHS I&A Open Source Collection Operations (OSCO) collected information regarding the unauthorized disclosure of unclassified FOUO I&A materials to two U.S. person (USPER) journalists. I&A personnel subsequently drafted three OSIRs that included attachments revealing the names of the journalists that posted the leaked information. These intelligence reports were unusual in that they reported on the activities of U.S. journalists engaged in ordinary journalism. I&A published the OSIRs following internal review. The national press discovered the OSIRs and reported that I&A had created and disseminated the intelligence reports, and characterized the reports' collection and publication as improper. The Acting Under Secretary of I&A (USIA), Mr. Brian Murphy, was subsequently detailed to a position in DHS outside of I&A on July 31, 2020.

This review determined that the release of the OSIRs is attributable to the following causes:

- a command climate that focused on discovering threats and immediately releasing "duty to warn" notifications and publishing OSIRs on those threats, which created a false sense of urgency for all OSIRs
- a poorly thought-out and insufficiently resourced reorganization and transition of Open Source Collection Operations to 24/7 operations
- the lack of a formal OSCO training program and disruptions to on-the-job training caused by the sudden increase in OSCO personnel and COVID-19 restrictions
- insufficient supervision of junior collectors caused by the excessive burdens imposed upon senior desk officers, which was exacerbated by the sudden increase in OSCO personnel and COVID-19 restrictions
- the deployment of untrained, inexperienced collectors to Portland
- improper collection tradecraft
- the pressure put on the Certified Release Authorities to review and publish OSIRs
- the decision to categorically unmask certain U.S. person information (USPI) against the recommendations of staff
- a poor staffing process for reviewing OSIRs prior to publication
- the faulty practice of identifying applicable collection requirements by viewing those listed on released OSIRs ostensibly concerning the same subject material

This review also examined the command and workforce climate at I&A. It found that Mr. Murphy created a toxic atmosphere at I&A as a result of his demeaning, dismissive and degrading treatment of I&A employees, and that many employees, to include senior personnel, continue to fear retaliation if he is reinstated.

[2] Ex. B48 (Email, Joseph B. Maher, SOPDUSIA to I&A Workforce, subject: "Internal Review", November 6, 2020 1:07 PM.)

This review examined whether any intelligence products were subject to politicization. No politicization was found; however, Mr. Murphy did attempt to controvert the raw intelligence collection process by directing collectors and analysts use a problematic term in intelligence reports which could have adversely colored finished intelligence products over time.

This review also considered whether I&A improperly exploited certain devices seized by FPS in Portland. I&A never exploited the devices. In fact, notwithstanding pressure from senior I&A leadership, including Mr. Murphy and the then-Acting Principal Deputy Undersecretary for I&A (PDUSIA) to exploit the devices, I&A staff correctly identified the standard for providing assistance to FPS and conveyed the requirements to FPS. FPS never attempted to fulfill the requirements (namely, to provide warrants for the seizure of the devices) or otherwise formally pursue a request for assistance.

Finally, in the course of the investigation, the review uncovered the practice of using Operational Background Reports (OBRs, colloquially "baseball cards") to create dossiers on USPERs arrested by federal authorities in Portland. Significant irregularities apparently existed regarding this practice given the collection, retention and potential dissemination of USPI regarding persons arrested for offenses seemingly unrelated to homeland security.

Based on the findings, the review makes the following recommendations, *inter alia*: conduct a holistic review of the strategic direction of I&A; improve training for Open Source Collection Operations (the section responsible for writing and releasing OSIRs); resolve and standardize unmasking rules for OSIRs; and conduct an in-depth review of various Current and Emerging Threats Center processes and standard operating procedures (SOPs).

## III. BACKGROUND

Beginning in late May 2020, a number of cities in the United States experienced increased incidences of general civil unrest following the death of George Floyd in Minneapolis. Although most participants in such civil unrest were engaged in peaceful protest, several cities experienced rioting, looting and more targeted violence and destruction against federal facilities, law enforcement officers and public memorials, monuments and statues (MMS). DHS personnel engaged in federal law enforcement response efforts in a number of cities, including Portland, OR.

The civil unrest in Portland became focused on the Justice Center. The demonstrations included targeted violence and destruction, including arson, of the federal courthouse located at Justice Center. DHS I&A received requests to collect information to support DHS personnel in Portland. Among other requests, DHS I&A's Current and Emerging Threat Center (CETC) Open Source Collection Operations (OSCO) was tasked with collecting open source information on the ongoing unrest in Portland by protesters planning to continue violence towards federal facilities or federal law enforcement officers protecting those federal facilities.

In late June 2020, in response to a recently issued Executive Order,[3] the I&A Intelligence Law Division (ILD) issued an internal guidance document titled "Job Aid: DHS Office of Intelligence

[3] Ex. B45 (Proclamation No. 13933, 85 Fed. Reg. 128, 40081 (July 2, 2020)).

& Analysis Activities in Furtherance of Protecting American Monuments, Memorials, Statues and Combatting Recent Criminal Violence."[4] The MMS Job Aid supplemented existing guidance on I&A's collection and reporting activities in the "context of elevated threats targeting [monuments, memorials and statues]; law enforcement officers, facilities, and resources and other government facilities" and specifically applied to "expanded intelligence activities necessary to mitigate the significant threat to homeland security articulated in the President's executive order of June 26, 2020." The Job Aid specifically reminded the collectors of the prohibition against engaging in intelligence activities for the sole purpose of monitoring activities protected by the First Amendment.

In response to unrest in Portland, OR, DHS deployed certain law enforcement personnel to aid in the protection of federal facilities. DHS I&A subsequently deployed personnel from its Field Operations Division (FOD) and OSCO to provide assistance to law enforcement personnel in Portland.

On July 20, the editor-in-chief of *Lawfare* published on social media a leaked copy of the Job Aid in an article raising alarms that DHS I&A was conducting unauthorized and unlawful intelligence activities on protesters engaged in activities (vandalism of statues) that had nothing to do with homeland security. That same journalist subsequently published on July 24 via Twitter a leaked email written by the Acting Deputy Under Secretary for Intelligence Enterprise Operations (ADUSIEO) on the topic of leaks, and the need to guard against leaks. This 'tweet' regarding the leaked email was reported in a CETC OSIR dated July 24 that included an attachment that identified the journalist, a USPER, by name.[5]

A second OSIR, dated July 26, included an attachment that included the same information regarding the same *Lawfare* reporter after he published on the same day a leaked email from the Acting USIA, Mr. Brian Murphy, that directed reports regarding Portland to use "Violent Antifa Anarchists Inspired" (VAAI) as a term of reference vice the previously approved term, "violent opportunists."[6] Finally, a third OSIR dated July 28, included an attachment that named a *New York Times* reporter, also an USPER, after he publicized a leaked DHS memo regarding DHS law enforcement involvement in the Portland protests.[7]

The three OSIRs were subsequently re-printed or quoted in a number of media reports alleging that DHS I&A was engaging in intelligence activities outside the scope of its mission and inconsistent with applicable intelligence collection and reporting laws and guidelines, as well as impugning the freedom of the press and lawful First Amendment activities. Mr. Murphy was temporarily detailed from I&A to a different position in DHS, and he subsequently filed a whistleblower complaint to the DHS OIG alleging that the detail constituted unlawful retaliation.

The media attention, temporary reassignment of Mr. Murphy and confusion regarding the scope of authorized collection activities in the context of long-duration mass protests associated with significant violence and destruction created substantial concern within the I&A workforce. In

---

[4] Ex. B46 (*Job Aid: DHS Office of Intelligence & Analysis (I&A) Activities in Furtherance of Protecting American Monuments, Memorials, and Statues and Combatting Recent Criminal Violence) (rescinded August 14, 2020)*.
[5] Ex. B10 (OSIR-04001-0932-20).
[6] Ex. B11 (OSIR-04001-0937-20).
[7] Ex. B12 (OSIR-04001-0952-20).

particular, media quotations from an unnamed source characterizing I&A as the "Junior Varsity" of the Intelligence Community generated a significant morale issue within the I&A workforce.

Following the media reports, the I&A Privacy and Intelligence Oversight Branch (PIOB) conducted a preliminary investigation to review the collection, retention, and dissemination of USPI regarding the activities discussed in the three OSIRs.[8] PIOB concluded that the collection and retention in question constituted a "questionable activity" and referred the matter to the DHS IG, which opened its own investigation.[9] The OIG's review of the matter remains on-going.

DHS received a number of requests for information from Congress related to the topics covered in this report. Production of documents and witnesses remains ongoing.

## IV. REVIEW

This investigation was initiated at the request of the Acting Secretary to the then-Acting General Counsel and conducted by five attorneys drawn from various DHS operational component legal offices outside of DHS headquarters.[10] Although the investigation began approximately on August 8, 2020, interviews did not begin until November 5, at the request of the DHS IG to delay any interviews during the pendency of its investigation. In addition to examining the circumstances that led to the release of the three OSIRs referenced above, this review also addresses the culture and morale of the I&A workforce. The investigatory team reviewed applicable documents and authorities and interviewed approximately 80 DHS employees.

## V. SUMMARY OF I&A AUTHORITIES AND RESTRICTIONS

I&A holds a unique position in the Intelligence Community as a domestic-facing intelligence organization supporting the homeland security mission. I&A's mission requires it to access and analyze threats emanating from within the United States and throughout the world, focusing on threats that could materialize in the homeland. Due to the domestic nature of many of DHS's missions, I&A is likely to collect, maintain, and disseminate information regarding USPERs and their activities within the United States, making understanding the constitutional, statutory and policy restrictions on intelligence collection integral to any discussion of I&A's authorities.

Three key authorities that explain I&A's proper collection, maintenance, and dissemination of intelligence regarding USPERs are the Homeland Security Act of 2002[11], the Privacy Act of 1974[12] (as amended), and Executive Order 12333 (as amended), which together define and establish the boundaries for I&A's intelligence activities.

The Secretary of Homeland Security, acting through designated DHS officials, has authority to collect, maintain, and disseminate information, particularly information relating to terrorism and

[8] Ex. B13 (*Preliminary inquiry into Open Source Intelligence Reports regarding U.S. Persons reporting on I&A activities*, (Aug. 5, 2020)).
[9] *Id.*
[10] One attorney each was assigned to this investigation from the Transportation Security Administration, U.S. Customs and Border Protection, and U.S. Coast Guard. The other two attorneys were assigned to this investigation from the Cybersecurity and Infrastructure Security Agency.
[11] 6 U.S.C. § 101 et seq. (as amended).
[12] 5 U.S.C. § 552a (as amended).

other threats to homeland security. The Secretary, acting through the Under Secretary for Intelligence and Analysis, is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other information in support of the DHS mission.[13] This authority advances DHS's primary mission[14] of counterterrorism as well as the Department's other homeland security responsibilities. However, while doing so, DHS must provide appropriate protections for the information and "protect the constitutional and statutory rights of any individuals who are subjects of such information."[15]

The Privacy Act provides statutory requirements for the maintenance, collection, use, and dissemination of information regarding United States Citizens and lawful permanent residents (together, U.S. Persons or USPERs), as well as civil and criminal remedies for violations.[16] The Privacy Act requires that each agency (including those engaged in intelligence activities) only maintain[17] information regarding USPERs if such information is "relevant and necessary" to fulfill its mission responsibilities.[18] In addition, the Privacy Act prohibits agencies from maintaining records that describe how USPERs exercise their First Amendment rights unless the subject of the record expressly consents; express statutory authorization exists; or the record is "pertinent to and within the scope of an authorized law enforcement activity."[19] In May 2019, Kevin McAleenan, then-Acting Secretary of Homeland Security emphasized this point in a policy statement to the Department, stating, "DHS does not profile, target, or discriminate against any individual for exercising his or her First Amendment rights."[20]

Executive Order (EO) 12333[21] establishes requirements for the Intelligence Community (IC) regarding the collection, retention, and dissemination of information concerning U.S. persons in part to protect USPERs' constitutional rights. Specifically, Section 2.3 provides that IC elements are authorized to collect, retain, or disseminate information concerning USPERs only in accordance with established procedures that have been approved by the Attorney General following consultation with the Director of National Intelligence. Those procedures are expected to include various categories of information, including among others, information that is publicly available, information needed to protect the safety of persons, and incidentally obtained information that may indicate activities in violation of law. These procedures are incorporated and implemented through IC directives, policies, and guidelines addressing the collection, retention, and dissemination of USPI.

---

[13] 6 U.S.C. § 121.
[14] *See* 6 U.S.C. § 111 (establishing the Department of Homeland Security and identifying DHS's primary mission).
[15] *See* 6 U.S.C. §§ 121, 482, 485.
[16] *See generally,* The Privacy Act of 1974, 5 U.S.C. § 552a.
[17] The Privacy Act defines the term "maintain" to include maintain, collect, use, or disseminate. 5 U.S.C. § 552a (a)(3).
[18] 5 U.S.C. § 552a (e)(1).
[19] 5 U.S.C. § 552a (e)(7).
[20] DHS Policy Statement 140-12, *Information Regarding First Amendment Protected Activities*, May 17, 2019. The point is also emphasized in a memorandum from Francis X. Taylor, then-USIA regarding protected speech in the context of protests. DHS I&A Memorandum, *Guidelines for Reporting on Protests and Constitutionally Protected Activities*, December 3, 2014.
[21] Executive Order 12333, United States Intelligence Activities, as amended, July 30, 2008.

The Department of Homeland Security *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines* (IO Guidelines),[22] govern I&A intelligence activities as they pertain to U.S. persons and provide guidance for DHS I&A "for the collection, retention, and dissemination of information concerning United States Persons," as required by E.O. 12333. The IO Guidelines were approved by the Secretary of Homeland Security and the Attorney General on January 11, 2017, and formally implemented within I&A pursuant to I&A Instruction 1000. The IO Guidelines recognize I&A's commitment to "delivering timely, actionable, predictive intelligence to its Federal, State, local, tribal, territorial, international, and private sector partners in support of the Department's national and homeland security missions."[23] This is balanced by the requirement that such activities are "conducted in a manner that is consistent with all applicable requirements of the law, including the Constitution, and that appropriately protects individuals' privacy, civil rights, and civil liberties."[24]

The Secretary, acting through the USIA, is authorized to produce and disseminate unclassified reports and analytic products based on open-source information in support of national and departmental missions.[25] The Secretary is also required to establish procedures on the use of intelligence information; to limit the re-dissemination of such information to ensure that it is not used for an unauthorized purpose; to ensure the security and confidentiality of such information; and to protect the constitutional and statutory rights of any individuals who are subjects of such information.[26]

In accordance with the IO Guidelines, I&A personnel are authorized to engage in the collection, retention, and dissemination of USPI where they have a reasonable belief that the activity supports one or more of the national or departmental missions. Reasonable belief is defined as

> A belief based on facts and circumstances such that a reasonable person would hold that belief. A reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge as applied to particular facts and circumstances, and a trained and experienced intelligence professional can hold a reasonable belief that is sufficient to satisfy these criteria when someone lacking such training or experience would not hold such a belief.[27]

Furthermore, acquisition of USPI must fall within one or more of the standard or supplemental information categories described in the Guidelines, e.g., consent, publicly available, foreign intelligence, counterintelligence investigative information, threats to safety, protection of intelligence sources and methods. Specifically prohibited by the Guidelines under all circumstances are any intelligence activities conducted "for the *sole purpose* of monitoring

---

[22] DHS I&A Instruction IA-1000, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines* (Jan. 19, 2017).
[23] *Id.* at p.1.
[24] *Id.*
[25] 6 U.S.C. § 121(d)(19). *See also generally id.,* at §§ 121, 122, 124a, 124h, and Ex. Order 12,333, §§ 1.7(i) and 1.11.
[26] 6 U.S.C. § 141.
[27] DHS I&A Instruction IA-1000, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (January 19, 2017) at Glossary-5.

activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States, or for the purpose of retaliating against a whistleblower or suppressing or burdening criticism or dissent" (emphasis added).[28]

Dissemination of USPI is only appropriate where it was properly collected and permanently retainable by I&A, is made to a proper recipient, and "[t]here is a reasonable belief that dissemination would assist the recipient of the USPI in fulfilling one or more of the recipient's lawful intelligence, counterterrorism, law enforcement, or other homeland security-related functions."[29] With the limited exception of certain circumstances not implicated here, in the absence of meeting all criteria for dissemination, the USPI may not be disseminated. Even when the dissemination of USPI is authorized, I&A must evaluate whether the USPI would materially assist the intended recipient in using or understanding it, and where it would not, the USPI must be anonymized (i.e., replaced with a generic marking, such as "USPER") before dissemination. Exceptions to the foregoing rule include instances when the USPI is publicly available, dissemination is authorized by consent of the person concerned, or the intelligence product or report originates from another IC element and is not materially authored or altered by I&A personnel.[30]

Per I&A Policy Instruction IA-900 Rev. 1, Official Usage of Publicly Available Information, only qualified Open Source Officers and Open Source Collectors are authorized within I&A to collect, retain, report and disseminate information or intelligence from publicly available social media platforms maintained and/or provided by non-Federal government entities.[31] The Instruction does not otherwise discuss limitations or additional oversight considerations regarding the collection of USPI. (Both DHS Instruction 264-01-006, *DHS Intelligence Information Report (IIR) Standards* and I&A Instruction IA-901, *Production of Finished Intelligence* discuss appropriate content and internal oversight review standards, but neither are applicable to OSIRs as OSIRs are neither finished intelligence products under IA-901 nor a form of raw intelligence reporting covered by Instruction 264-01-006 (which is applicable only to IIRs.)

A number of Intelligence Community Directives (ICDs) also govern treatment of USPER information, and Executive Order 12333 prescribes specific instances when collection, retention, and dissemination of USPER information is permissible. Most notably, ICD 107, Civil Liberties, Privacy, and Transparency, establishes the policy for protecting civil liberties and privacy and for providing greater transparency. It requires the Head of an IC Element (HICE) to "[c]onduct intelligence activities in a manner that protects civil liberties and privacy and provides greater public transparency."[32] Additionally, the HICE shall "[e]nsure that Privacy and Civil Liberties Officers, General Counsel, Inspectors General … have access to all information required to protect civil liberties and privacy and to provide greater public transparency."[33] IC

[28] *Id.*
[29] *Id*. at § 2.3.1.
[30] *Id*. at § 2.3.5.
[31] *See* DHS I&A Policy Instruction IA-900 Rev. 1, Official Usage of Publicly Available Information.
[32] ICD 107, Civil Liberties, Privacy, and Transparency (Feb. 28, 2018) at E.3.a.
[33] *Id.* at E.3.e.

employees and those acting on behalf or in support of an IC element must also responsibly protect civil liberties and privacy and provide greater public transparency.

## VI. FINDINGS

### A. The Current and Emerging Threats Center (CETC) was Unprepared for the Mission Assigned.

Under USIA Glawe and PDUSIA Murphy, I&A intelligence operations shifted focus from strategic collection, analysis and intelligence to an operational function supporting law enforcement activities. CETC was a microcosm of this I&A shift. This abrupt mission focus change across I&A did not thoroughly consider the existing duties of I&A, or the capabilities and frailties of the institution. The move to transform I&A to meet a completely different mission set was acutely felt within the newly-created CETC where changes exacerbated structural problems within the elements that made up the division.

CETC was built out of the former Collections Division, itself divided during former USIA David Glawe's reorganization of I&A into mission centers.[34] CETC received the open source collectors, the request for information (RFI) management system, and the Watch.[35] Each of these sections underwent a poorly managed and under-resourced reorganization process that created the potential for future questionable intelligence activities. Ultimately, the transformation of CETC to focus entirely on current and emerging threats on a 24/7 basis upended the previously small informal organization, removed institutional guardrails, and failed to provide the necessary resources for sustainable growth or mission success.

#### 1. The Open Source Collection Operations (OSCO) Transformation

Prior to 2018, OSCO was a smaller organization with senior collectors on a maxi-flex schedule covering 0430 to 1930, limited middle management, and a team of about six federal employees and six contractors.[36] OSCO collected to support all DHS missions, and collectors had defined portfolios and subject matter expertise.[37] The structure of this office changed to meet CETC's new focus on imminent and direct threats that resulted in a duty to warn.

##### a. Threat Notifications and the Move to 24/7 Shifts

This shift in collection focus began in 2017-18 with I&A's support to ICE when a number of protests against ICE policies and activities nationwide, coincided with an increase in the number of threats against ICE personnel. OSCO surged to support ICE by seeking any and all threats to ICE, in products known as "Threat Notifications."[38] OSCO's reporting instructions included all

[34] Ex. A44.
[35] *Id.*
[36] Ex. A15, A35, A45, A58.
[37] Ex. A35, A45, A58, A74.
[38] Ex. A2, A4, A15, A35, A55.

threats to ICE, regardless of how spurious or general the threat.[39] Additionally, then PDUSIA Brian Murphy had directed that OSCO stop masking USPI [40] and instructed I&A personnel to include source information in the first paragraph of OSIRs.[41] These changes resulted in a deluge of reporting, creating a precipitous decline in adherence to content management standards to release the reports. The recall rate for OSIRs increased from two the previous year to 30.[42] The surge in threat reporting to DHS personnel and facilities "demonstrated the value of open source," according to Mr. Glawe, who then pushed for the expansion of OSCO to 24/7 operations after presentation of OSCO threat reporting statistics during this time period.[43] A placemat that was created by the then head of CETC to demonstrate CETC's successes highlighted the value of "duty to warn"[44] notifications from CETC.[45] Prior to the support to ICE, the "duty to warn" was not a collection focus in and of itself, but rather an occasional incidental duty to collectors otherwise responding to other intelligence requirements.[46]

Moving forward, OSCO would transform into a 24/7 organization focused on on-going threats generally, with a main goal of providing threat warnings to federal, state, local, tribal and territorial law enforcement. The move to 24/7 operations in the fall of 2018,[47] began a trend of personnel turnover that continues to plague OSCO, resulting in a massive influx of new hires in a very short period of time.[48] To meet the change to 24/7 operations, I&A leadership initially planned to surge employees from the rest of I&A, but this plan was deemed unsustainable, so OSCO received federal billets to staff 24/7 operations in shifts.[49] OSCO ballooned in size, growing by 200% to 32 federal employees.[50] Prior leadership did not consult with staff on these changes in direction or organization.[51] Additionally, to enable this new focus on threat reporting, the collectors' portfolios, which varied from foreign terrorism to transnational organized crime to cyber, were largely eliminated.[52] Horace Jen, Deputy Undersecretary for Intelligence Enterprise Operations (DUSIEO), told the Director of CETC to make subject-matter portfolios at most 20% of the activity at OSCO,[53] but by 2020 by the estimate of the Branch

[39] Ex. A15, A55.
[40] Ex. A2, A15. Contrary to staff recollection, Mr. Murphy states this direction came from Mr. Glawe. Ex. A46.
[41] Ex. A35.
[42] *Id.*
[43] Ex. A19, A58.
[44] Duty to warn is a requirement under ICD-191 and IA-105, which requires I&A to warn a subject and law enforcement of a threat when it "acquires credible and specific information indicating an impending threat of intentional killing, serious bodily injury, or kidnapping directed at an intended victim." IA-105 sets out criteria to determine the credibility of a threat requiring the collector to have reasonable belief and specific information about the threat, location, and victim among other information. Ex. B7, ICD-191, *Duty to Warn* (July 21, 2015); B8 (IA-105, *DHS Intelligence and Analysis Duty To Warn* (Nov. 28, 2018)). Neither ICD-191 nor IA-105 require I&A to collect or actively seek out direct threats to individuals, but if such direct threats to persons are found, then I&A provides warnings. *Id*.
[45] Ex. A19.
[46] Ex. A2, A54, A63, A75.
[47] Ex. A19.
[48] Ex. A15, A35, A37, A58, A64.
[49] Ex. A19.
[50] Ex. A58.
[51] *Id.*
[52] Ex. A15, A19, A37, A50.
[53] Ex. A58.

Manager of OSCO, OSCO's reporting was 95% threats.[54] These changes resulted in approximately half of the federal employees assigned leaving to avoid shift work, to maintain their work life balance, or because they disagreed with the new mission direction of CETC.[55] The exodus of experienced personnel with institutional knowledge and unique skills created follow-on issues including a lack of on-the-job trainers required for the influx of new employees.

b. Uneven Growth in OSCO Created Bottlenecks in OSIR Production and Overstressed Senior Employees.

CETC ultimately received 32 billets to conduct its OSCO mission - four desk officers/senior collectors, two branch chiefs, 24 collectors, and two supervisors/content managers.[56] These billets were drawn from across the agency, but were fewer than what CETC leadership thought would be necessary to successfully staff a 24-hour center.[57] Prior to OSCO's expansion, it had two content managers whose sole duties were to review and publish OSIRs. Neither of these content managers possessed previous open source collection experience, but both were intelligence professionals with extensive experience reviewing and writing serialized reports.[58] Before OSCO expanded, the two-person capacity was enough to quickly and efficiently review and publish OSIRs.[59] However, OSCO's expansion did not include an expansion of reviewers.[60] The most senior content manager, who built and maintained the OSIR management and publication software tool (HOST), left due to overwork.[61] CETC leadership responded by elevating the previous other content manager and a senior collector into a newly-created senior desk officer (SDO) role.[62]

Immediately following their promotion, the SDOs were quadruple-hatted, having to review and publish all of the OSIRs across all three shifts, supervise and manage all the collectors, oversee training of new collectors, and maintain and support HOST tasks.[63] Content managers had to execute all four of these responsibilities for 200%[64] more collectors than had previously assigned to OSCO. Furthermore, the collectors reported at a much higher operational tempo on generalized threats and were now working on a 24/7 basis. Both content managers struggled to use HOST's antiquated and byzantine processes,[65] which were purposely designed to be labor intensive to ensure quality control.[66] This overwhelmed the new SDOs who, on top of their two operational duties, also had to supervise a staff of largely new federal employees. The SDOs were themselves first time supervisors with no specific supervisory training.[67] The SDOs'

[54] Ex. A50.
[55] Ex. A35, A58, A75.
[56] Ex. A58.
[57] Ex. A10, A58.
[58] Ex. A35, A64.
[59] *Id.*
[60] Ex. A58.
[61] Ex. A35.
[62] Ex. A58.
[63] Ex. A22, A58, A64.
[64] Arguably this is a 400% increase given that the previous contractors were supposed to have arrived trained. Ex. A48.
[65] Ex. A58, A64.
[66] Ex. A35.
[67] Ex. A35, A64.

inability to simultaneously publish OSIRs and supervise created a backlog of OSIRs.[68] The backlog required recalling a former senior content manager multiple times back to OSCO after he had moved on to a different job,[69] and created a perception by the workforce that their performance was not monitored.[70] The sheer number of OSIRs, coupled with the exhausted SDOs, led to a marked decrease in OSIR quality control,[71] and put greater stress and emphasis on the initial peer review of OSIRs.

Prior to the end of the Portland deployment, publication of an OSIR required peer review before submission to the overworked SDOs. However, those peers had themselves only been at OSCO for a limited amount of time.[72] Since the Portland deployment, OSCO has implemented a desk officer (DO) role that is a non-supervisory GS-13 team lead,[73] who is a second line of review after the initial peer review.[74] Many of these DOs are more experienced collectors, but this is not universally true.[75]

The OSCO Branch Chief has stated that they could not bolster the review side of OSCO because the position of SDO requires open source collection experience, which is hard to find.[76] However, one of the current SDOs has no open source collection experience and the most effective content manager prior to the reorganization also had no open source collection experience, but did have other intelligence reports, collection, and review experience.[77] Additionally, OSIRs are modeled after Intelligence Information Reports (IIRs), which use a standardized format for raw intelligence reporting used across the Intelligence Community.[78] As such, a quite large pool of intelligence professionals should exist who may not have open source experience, but would have other raw intelligence experience to enable him or her to understand how to review raw reporting for thresholds, intelligence oversight (IO), content, and style.

Resources were another constraint. The CETC Director approached the then-PDUSIA for more billets, but this request was not elevated to higher leadership because those billets would have to come from somewhere else in I&A.[79]

These bottlenecks persist and are a factor in how the improperly collected and disseminated OSIRs were produced. At the time of this report, a backlog of OSIRs await review, to the point that many of them will never be actioned.[80] Not only does the intelligence go stale, the backlog also has had a negative impact on morale. Many collectors are unsure why they are collecting since their reports are not being disseminated in a timely manner.[81]

---

[68] Ex. A35.
[69] Ex. A35, A50.
[70] Ex. A21, A30, A41, A43.
[71] Ex. A35, A64.
[72] Ex. A37.
[73] Ex. A20.
[74] Ex. A34.
[75] Ex. A15, A20.
[76] Ex. A50.
[77] Ex. A58.
[78] *Id.*
[79] *Id.*
[80] Ex. A41, A64.
[81] Ex. A37, A43.

### c. CETC's Lack of a Formalized Training Program Crippled its Workforce and Engendered Poor Performance.

When OSCO moved to 24/7 operations, the influx of new personnel, the exodus of senior collectors, and the lack of a formal training structure or SOPs for collectors essentially left the untrained training the untrained.[82] OSCO historically relied on a practice of on-the-job-training (OJT), as opposed to a formalized training program;[83] however, the rapid expansion of OSCO's workforce amplified the training deficiencies inherent in OSCO's training process.[84] As a result, OSCO's training model became unsustainable once I&A made the decision to greatly expand OSCO's operations due to the relative lack of trainers to conduct OJT.

Prior to the Portland OSIR incident, the OSCO training model was as follows: When new hires arrived at OSCO, they underwent a week-long training course introducing them to the general structure, policies, and standards of DHS as an agency.[85] A second week consisted of I&A specific training familiarizing them with I&A policies and procedures, including the intelligence oversight training which, up until recently, was provided only online via PALMS.[86] During their third week at the agency, the newly hired collectors attended a three-day open source intelligence course developed and delivered by ITA, and then finally the collector was paired with a more experienced or seasoned collector for OJT where they would spend the next three to four months rotating through experienced collectors until they became sufficiently proficient to begin collection activities on their own.[87] Ideally, the OJT training model can be extremely beneficial, as it is a generally accepted principle that individuals learn best through direct demonstration or actively performing the task themselves. This model is most effective in a live environment. When done virtually, however, it can engender some significant operational inefficiencies and inadequately trained personnel, as was the case in the months leading up to events in Portland.[88] As noted below, during the early days of the COVID-19 pandemic, the standard CETC training model was unavailable for training the new hires because so much of the work force was working remotely.

One key training aspect missing from this training paradigm is live intelligence oversight training. Intelligence Oversight (IO) training is a critical piece of the National Intelligence

---

[82] Ex. A37, A43, A75.

[83] As the CETC Director noted, "there is no directed course on collection" even though he has expressed the need for a collections focused training to the Intelligence Training Academy (ITA), an organizational need that has been unmet since 2014. Ex. A58. ITA does provide a three-day Open Source Intelligence (OSINT) course among several other courses such as the Basic Intelligence Training Course. Ex. A68. ITA's mission is to serve the training needs of I&A as well as that of the greater DHS Intelligence Enterprise. Ex. A1, A46, A68. (ITA also services state and local governments though priority for courses is given to DHS Intelligence Enterprise employees. Ex. A1, A46, A68.) ITA develops curriculum and delivers the training; however, it does not create certifications, set employee course requirements, or establish tradecraft standards. This responsibility rests solely with the mission centers. Ex. A1.

[84] Ex. A27.

[85] Ex. 30, A50.

[86] Ex. A2, A26, A50, A58.

[87] Ex. A27, A35, A45, A50, B23 (Email Action DUSIER to Acting DUSIEO, RE: Please review – prelim review, August 3, 2020 9:38 AM).

[88] I&A has substantially enhanced CETC training since the Portland incident.

Program. It educates members of the IC on their authorities and constraints on those authorities, their obligations as members of the IC, and the laws and policies providing individual privacy protections to USPERs. Historically at I&A, the IO Office delivered this training live during the onboarding process. However, for reasons unclear, the IO Office was asked to reduce its training segment to just 30 minutes. The IO Office thought 30 minutes did not provide adequate training time to properly cover the crucial aspects of intelligence oversight. Consequently, the IO Office declined to provide a 30 minute segment and the virtual intelligence oversight course provided on PALMS replaced the live oversight training piece.[89] Despite the online intelligence oversight course that new hires are required to complete, a number of witnesses questioned could not identify DHS I&A IA-1000, also referred to as the Attorney General or Intelligence Oversight Guidelines, nor were they familiar with its contents.[90] After the Portland incident, intelligence oversight training was reinstated as part of "live" employee orientation training.[91]

COVID-19 presented a particular challenge for OSCO. OSCO began ramping up operations and increasing its workforce from 12 employees to 32 at the same time the COVID-19 pandemic engulfed the nation, sending much of the federal workforce home to telework. By mid-March, most of OSCO was teleworking and OSCO had to institute a virtual training plan for its then four new hires.[92] The junior collectors were instructed to complete on-line trainings provided by DHS, some of which included PALMS and a McAfee[93] training, among others. Most of the training only had a tangential relationship to open source collection and was not especially helpful. Several persons interviewed shared a common sentiment by stating that "these trainings were geared to law enforcement or deployed military personnel who work in more permissive environments."[94] Additionally, the collectors were advised to review the OSCO Cookbook, an open source collection procedures guide authored by a former CETC employee.[95] Most collectors found this guide to be "outdated, not comprehensive, and lacked real life examples."[96] It was not "very useful or practical" and although it provided "some practical technical information, like avoiding special characters," it lacked "guidance on substantive issues. For example, the cookbook does not have guidance on First Amendment considerations.[97]

Indicative of the friction and difficulties introduced into training new hires, at least one new hire was apparently neglected for almost a month. From the time her employment began in May until sometime in June, this collector focused entirely on on-line training, completing unrelated training provided by DHS that "had nothing to do with her job at OSCO."[98] No one from CETC reached out to this collector during this time period, then suddenly as OSCO began to surge for a crisis event, she was paired with a more senior collector who apparently was overworked and received little notice that she had to train a junior collector. While shadowing this senior

[89] Ex. A2.
[90] Ex. A38, A41.
[91] Ex. A2.
[92] Ex. A21, A30, A50, A72.
[93] McAfee training is more than IT security. McAfee also provides Open Source Collection training. *See* https://www.mcafeeinstitute.com,
[94] Ex. A6, A30, A34.
[95] Ex. A35, A37, A43.
[96] *Id*.
[97] Ex. A6, A45, A47.
[98] Ex. A21.

collector, the surge crisis left little time for the junior collector to receive adequate training. Consequently, she possessed limited knowledge regarding open source collection when she was tasked with writing her first OSIR. She resorted to reaching out to another newly hired collector to walk her through the process of drafting an OSIR.[99] She also reviewed other previously written OSIRs as a guide on how to write an OSIR, a method most other collectors resorted to when they first started.[100]

Constrained by COVID, the training program came to an almost complete halt. The junior collectors found themselves often having to rely on each other as a resource.[101] One junior collector complained that "it's overwhelming to sit by yourself and self-teach," and that she did not like operating like this.[102] As one collector explained, "on the job training worked okay when you are in an office environment, you had someone you could reach out to. But when COVID hit, everyone went remote. So now you are isolated trying to do the job, even though you can reach out to ask questions, but it's different since it's not as easy as reaching out to someone right next to you."[103] The pandemic and the surge greatly impaired OSCO's ability to follow its traditional three to four month OJT schedule for new hires.

Almost all training, DHS Headquarters on-boarding training, even training to become a Certified Release Authority, was on hold due to COVID.[104] ITA training went on a five-week hiatus as it feverishly worked to transition its live training courses to a virtual environment.[105] In late May, OSCO was offered additional resources through a joint duty assignment (JDA) with CISA employees, but OSCO apparently declined. As noted by the OSCO branch chief, it was hard enough trying to train their own collectors remotely, and bringing on JDAs at that time would have only added to their struggles.[106] Adding further aggravation to an already incredibly strained system, OSCO was required to surge to respond to crisis events that arose as a result of the George Floyd killing. New hires, who had barely received any form of training, were immediately activated to assist in any capacity possible. A scrambled purchase for laptops was made through acquisitions from Best Buy, and on a Saturday evening, the new hires were asked to meet in the DHS Nebraska Avenue Complex (NAC) parking lot so they could pick up a "collection" laptop.[107] The OSCO branch chief, via Microsoft Teams Chat, then walked them through downloading the necessary software and visiting social media sites to collect information.[108] Two witnesses complained that they and others who were given equipment were not provided the appropriate operational security measures (a virtual private network (VPN) or a managed attribution tool) on these "collection" laptops to protect their privacy. Without these

[99] *Id*.
[100] Ex. A21, A37, A41.
[101] *Id.*
[102] Ex. A15.
[103] Ex. A35.
[104] Ex. A58.
[105] Ex. A1, A42, A68.
[106] Ex. B24 (Email, OSCO Branch Chief to CETC Director, subject: FW: OSCO Surge still needed?, Tuesday May 26, 2020 1:54 PM).
[107] Ex. A50.
[108] *Id.*

tools, they believed that they were vulnerable to any nefarious actors looking to expose their private information, doxx DHS personnel, or invade the employee's home network.[109]

The junior collectors were instructed to scan social media platforms and to take screen shots of threats to send to senior collectors for review and possible OSIR drafting.[110] After a week or so of doing this, the junior collectors began writing their own OSIRs and conducting peer review of other drafted OSIRs, in spite of not being sure of all the criteria and requirements at that point.[111] "They received guidance on how to write OSIRs by calling different collectors and asking them how to do the various parts."[112] In fact, "the new collectors started a group chat for themselves where they could share how things were going."[113] Despite CETC leadership warning I&A leadership that the collectors were inexperienced and not properly trained, CETC leadership was told to "surge anyways," and to "make it work."[114]

Other CETC employees and those belonging to other mission centers did not appear to have the training issues that affected OSCO.[115] The Watch's training paradigm mirrors that of OSCO. New hires must undergo the two-week general employee orientation with greater DHS and then I&A, but when they arrive at CETC, Watch employees have several draft SOPs that serve as references. The junior watch standers receive on-the-job training just like OSCO personnel, but due to the nature of the duties watch standers carry out, the Watch's OJT model seemed to be more effective, although some improvement is warranted.[116] Another possible explanation for the disparity in training efficacy is that the Watch did not undergo a massive expansion like OSCO where it needed to train twenty new hires at the same time. Both the OSCO and the Watch's training models are predicated upon absorbing one or two new hires at a time. Some watch standers complained that the training was inadequate.[117] At least one watch stander attended the Intelligence and Analysis Basic Course three months after his employment with CETC began.[118] Within the Watch, a new hire also receives a checklist of items they need to perform, specific trainings and tasks.[119] The Watch implemented this checklist requirement about a year ago. Similarly, OSCO has a checklist new collectors must complete, though it is

[109] Ex. A26, A75, B25 (Email to staff, subject: RE: Concerns from CETC, Friday June 5, 2020 5:20 PM).
[110] Ex. A34, A52.
[111] Ex. A43, A52.
[112] Ex A52.
[113] *Id.* This group was called, "New and Confused." Ex. A43.
[114] Ex. A48, A50, A58. Mr. Murphy alleges that he never heard push back on training issues or not being able to complete tasks at CETC due to a lack of training. Ex. A46. One collector attended an OSINT conference using her own funds to buy her ticket. At the conference there were tabletop exercises and competitions. The collector opined that "many of the [OSCO] collectors, even the senior ones, were clueless about the rest of the field or social media." She explained, for instance, when "(b)(3)(A)(ii) [redacted] that impacted their collection no one in leadership knew what to do or what an (b)(3) was." "Everyone is clueless about the basic things in the field of OSINT." This collector's request to attend a DHS I&A 101 course was denied. Ex. A43.
[115] Per Mr. Murphy, OSCO did not have a lack of training, and he never saw anything that indicated OSCO was not getting the training that they needed, but he also stated that he had limited knowledge of OSCO's training program and was unable to describe it. Ex. A46.
[116] Ex. A7, A23, A32, A55, A66.
[117] Ex. A61.
[118] Ex. A66.
[119] Ex. A39.

unclear when this checklist was developed and became available.[120] At least one OSCO employee advised that she was provided with a checklist about one month after she started.[121] As the civil unrest intensified and OSCO collectors questions and concerns increased about the legal parameters of their collection activities (beyond references to the Cookbook and the Intelligence Oversight Guidelines), CETC offered no other resources to its employees. In contrast, FOD invited ILD, IO, and CRCL to provide training to its personnel.[122]

A major deficiency in the deployment of OSCO personnel to Portland was the deployment of inexperienced, inadequately trained junior collectors without any sort of pre-deployment training offered to help address their underdeveloped understanding of true threats, First Amendment protections, collection requirements, and national intelligence and DHS departmental mission sets.[123] Instead, the Portland team only received a quick counterintelligence briefing and a gas mask with rudimentary instruction just a few hours before they deployed. The Portland team received only a 24-hour notice that they would deploy.[124] On or about July 28, 2020, the need arose to rotate some of the collectors out from Portland and replace them with new volunteers. In the announcement, a CETC supervisor solicited collectors who were "preferably fully trained, but will consider others based on where you are in training."[125] By this time, the offending OSIRs had already been published, drafted by a junior collector on the Portland team. Regarding his training, this collector stated, "aside from the cookbook and a couple of emails about the threats to look for, I was not given guidance about what to collect before I began collecting."[126] There was no brief provided by ILD or the IO Office to OSCO personnel, although apparently such a briefing was provided to other mission center employees that deployed, perhaps at the request of the Directors of those mission centers.[127]

d. Impact of Poor Training**.**

The impact of CETC's poor training program created deficiencies in the collectors' understanding of collection requirements, I&A's mission as a strategic intelligence agency, the support elements available to CETC personnel, and tradecraft.

A number of collectors interviewed demonstrated a poor understanding of the collection process, most notably the order of a collection activity itself. Ideally, a collector starts by identifying the mission sets for the intelligence element and reviews the collection requirements drafted to support those mission sets. With the collection requirement in mind, the collector then embarks

[120] Ex. 50.
[121] Ex. A35. The training provided to FOD personnel additionally underscores the inadequacies in CETC's training program. FOD personnel have specific field intelligence review and raw intelligence review release courses that they take as part of their formal training program. These courses were taught by ILD, IO, PRIV, and CRCL (colloquially referred to as the G4). In addition, they learn trade craft by attending courses such as Analysis 101, provided by ODNI. Ex. A11.
[122] Ex. A9.
[123] Ex. B26, Internal I&A AAR, Civil Unrest/Violence AAR – Findings and Questions for Senior Leadership, undated.
[124] Ex. A30, A43, A52, B27(Email, OSCO Branch Chief to staff, subject: Meeting at 1300 at the NAC, Thursday, July 9, 2020, 10:26 AM.)
[125] Ex. B28 (Email, OSCO SDO to OSCO staff member, subject: Re: Portland, Tuesday, July 28, 2020 10:24 PM).
[126] Ex. A52.
[127] Ex. A43.

on his or her collection activity in pursuit of information to satisfy that collection requirement. The issue with the threat-based focused searches is that the collection requirement is so broad, that the boundaries of the search are not well-defined. Furthermore, when the emphasis is on finding threats to the Homeland or threats to law enforcement, the collectors become accustomed to using only those two collection requirements. If other information of value arises that is not a threat, they would then try to locate a collection requirement to fit the information garnered.[128] Support to mission centers appeared as a secondary consideration to "finding something" while collectors engaged in this collection process.[129]

In the case of the three OSIRs that were leaked and are at issue in this investigation, a junior collector stumbled across the information of the leaked DHS material, and with an understanding that a leak of unclassified DHS information was a significant concern of the Department,[130] mistakenly believed that the leak warranted production of an intelligence report.[131] Several individuals who were interviewed, including CETC's Director and OSCO's Branch Chief, believed that a leak of unclassified information by a USPER with no foreign connection fit under the counterintelligence umbrella.[132] Counterintelligence (CI) as defined in E.O. 12333 means "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations c*onducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities*."[133] Remarkably, less than five witnesses asked were able to specify a foreign connection in the definition of counterintelligence.[134] CETC's former Acting Director and current director of the CI Mission Center, indicated that she would be surprised if OSCO was relying on a counterintelligence collection requirement for the OSIRs drafted on leaks of unclassified information – "CI collection requirements would not be relevant unless there was some sort of foreign adversary involved."[135] There was no suspected involvement of a foreign adversary with respect to the three OSIRs at issue, which involved the unauthorized release of information to an USPER member of the media. Nonetheless, many CETC employees appeared to erroneously believe a CI nexus existed. Several appeared to be confused about how to report an unclassified leak and some were not aware that a leak needed to be reported to the Chief Security Officer, or that DHS even had an insider threat program.[136]

Similarly, collectors were confused as to what constituted a "true threat" despite an I&A ILD memo that discussed distinguishing between hyperbole and a reportable threat.[137] During the surge concerning Portland, one CETC employee suggested that "some front end training of what is or is not a threat should be explained in detail to all new collectors."[138] Apparently, this

[128] Ex. A35, A36, A43.
[129] Ex. A43.
[130] Ex. A6, A14, A17, A21, A24, A28, A52, A56, A76.
[131] Ex. A52.
[132] Ex. A50, A58.
[133] E.O. 12333, § 3.5(a) (emphasis added).
[134] Ex. A40, A41 A50.
[135] Ex. A19.
[136] Ex. A41, A50, A55, A58.
[137] Ex. B9 (Memorandum from the Intelligence Law Div. on Social Media Statements Referencing Violence Against or Doxxing of DHS Personnel and Facilities, July 13, 2018).
[138] Ex. B29 (Email, CETC Director to staff, subject: Re: Current Process for Publishing, Saturday, August 1, 2020 1:36 PM).

suggested training did not occur. The content managers remained responsible to ensure only reportable threats were published against a backdrop of increased emphasis on quantity versus quality that exacerbated the misinterpretation of the ILD guidance memo and confusion over what characterized a "true threat." With regard to tradecraft, one collector expressed that on several occasions, unlike his other experiences in the intelligence community, he found that I&A did not possess well-developed and standardized "tradecraft." Instead, he thought that I&A/CETC staff seemed to rely very much on "individualistic experience" which led to a lot of variation in work product from collector to collector.[139]

Another example indicative of poor training was identification of sources. Many junior collectors would find a new source and use the information without properly considering the source's historical activities, such as past comments made, other violent or crime-related interests, links to nefarious groups, previous violent actions or incitements to violence.[140] Instead, it was a "one and done" type of review – if the source made one threatening statement like "kill cops," that statement sufficed for a report without regard to that subject's "prior anti-law enforcement sentiment" or propensity to intentionally incite violence or commit a violent act.[141] To clarify, someone saying "we should kill cops," could be exercising First Amendment protected speech, and reporting on that could violate DHS First Amendment Policies. On the other hand, a directed message encouraging certain people to meet up at a specified time and place to kill cops would be treated differently. These distinctions underscore why a solid understanding of the intricacies involved with the intersection of First Amendment policies and intelligence collection activities is imperative. The apparent failure of I&A leadership to recognize the challenges inherent with these seemingly small differences, and the attendant failure to implement proper training to address these issues, played a large part in the failures at Portland.

e. The Pressure to Quickly Report All Threats Induced Improper Collection and Dissemination.

The move to change the focus of OSCO to collect primarily on "duty to warn" threats came with dual pressures – pressure to report and pressure to disseminate as quickly as possible in order for law enforcement to take action. Searching for true threats of violence before they happen is a difficult task filled with ambiguity. For example, in 2018, the Tree of Life Synagogue Shooter posted online prior to engaging in violence, "I can't sit by and watch my people get slaughtered. Screw your optics, I'm going in."[142] The shooter posted the statement hours before committing murder. The "flash to bang" of events has been dramatically reduced into days, minutes, or even seconds.[143] While preventing violence is a noble goal, the pressure to provide "anticipatory" or "predictive"[144] intelligence led to collection of a broad range of general threats that did not meet

[139] Ex. A20.
[140] Ex. A35, A45.
[141] Ex. A45.
[142] Robinson et al., *11 Killed in Synagogue Massacre; Suspect Charged With 29 Counts*, N.Y. Times (Oct. 27, 2018), https://www.nytimes.com/2018/10/27/us/active-shooter-pittsburgh-synagogue-shooting.html.
[143] Ex. A46.
[144] Ex. A45.

the threshold of intelligence collection[145] and provided law enforcement and intelligence partners with information of limited value. OSCO collectors are tasked with a difficult mission – identifying and collecting on threats to homeland security conveyed online.[146] By their nature, identifying and taking action on those threats for intelligence reporting is challenging.[147] In fact, had the social media statement the Tree of Life Synagogue shooter posted less than an hour before his attack – "screw your optics I'm going in" – been discovered before the event, it likely would have been too vague to even meet the threshold for collection in furtherance of I&A's domestic terrorism mission or constitute a duty to warn under IA-105.[148]

Regardless, pressure existed to prevent and to anticipate potential violence from CETC and I&A leadership.[149] Every report became a priority since all materials that OSCO collectors were reviewing and collecting were supposed to be threat-based. This pressure translated to a high operations tempo to ensure that these perceived threats were timely reported. The pressure was put not only on the collectors, but also on the SDOs to speed up their reviews and publish OSIRs.[150] This, coupled with the fact that the OSCO collectors were primarily graded on the average number of OSIRs they produced a month,[151] pushed limited review of the threats they collected. However, since a majority of the collectors were new and were often trained by equally inexperienced collectors, their primary method to find threats was to search using key words of their choosing and then use the "threat collection requirement" to justify what they had found rather than to use collection requirement to guide their searches. A former content manager stated that collectors were like a "bunch of 6th graders chasing a soccer ball – everyone wanted to be the collector who found the golden egg or found the threat."[152] Collectors during this period collected on any threat, even from those that appeared to be unlikely or from profiles with no other postings or information,[153] hoping to stop the next Tree of Life shooter. The CETC Director did not want to be scooped by other organizations,[154] and would get excited

[145]"I&A personnel may collect and report on social media and other publicly available sources where they have a reasonable belief that these activities assist the Department in identifying protective and support measures regarding threats to homeland security , including where they have a reasonable belief that the activities would (1) constitute "true threats" to or incite violent acts' against DHS personnel or property, (2) provide analytically significant insights concerning an individual reasonably believed to pose a threat to DHS personnel or property, (3) in certain cases, inform an overall assessment of the risk of violence against DHS personnel or property, or (4) expose private or otherwise identifying information about DHS personnel or facilities (i.e., doxxing), which, while not a threat per se, might result in a downstream threat of violence, including domestic terrorism, or otherwise prevent DHS from executing its lawful mission." Ex. B9 (Memorandum from the Intelligence Law Div. on Social Media Statements Referencing Violence Against or Doxxing of DHS Personnel and Facilities, July 13, 2018).
[146] Ex. A25.
[147] *Id.*
[148] Ex. A25, A41.
[149] Ex. A45, A46.
[150] Ex. A50.
[151] Ex. A58
[152] Ex. A35.
[153] This practice of single use sources was contrary to traditional tradecraft in open source collection, where one generally wants a source with good placement and access that one can reuse, and presumably, lead to other new sources with knowledge of the subject area under examination. Ex. A15, A35, A45. Additionally, evaluating a source to see if there are other threats views or connections can help determine the trueness of a threat. *Id.* By 2020, CETC had increased to over 2500 sources, up from 200 sources in 2017. Ex. A35.
[154] Ex. A55.

about information, wanting to publish as soon as possible.[155] Additionally, many members of the staff and the CETC Director noted that they did not know who needed to know the threat information, and so they often distributed the information as widely as possible.[156]

The speed and volume of reporting created mixed operational results. Immediate threats were posted into an FBI managed system, eGuardian, that alerted the FBI and State, Local, Tribal, and Territorial (SLTT) partners and allowed them to conduct further investigation.[157] The threat would also be disseminated in an OSIR. Initially, the Watch[158] received complaints from the FBI about the "crap" being sent through eGuardian because the FBI would have to investigate each threat.[159] The CETC Director stated that this problem with the FBI was a matter of growing pains into the new role and that CETC no longer receives complaints from the FBI on eGuardian matters because more stringent standards for posting exist.[160] However, this focus comes at a cost to supporting other I&A mission space and likely has little impact on responding to threats of violence in the United States. Threats of violence were not a focused collection effort previously because of the massive "criminal activity, violence, things going out there," and that I&A, "would not put a dent in it."[161] Given that DHS and DOD are the primary readers of OSIRs, whether law enforcement acts on the information is unclear.[162] At best, anecdotal evidence exists of threat reporting's value to SLTT and the FBI,[163] but there is clear evidence that OSIRs are no longer being utilized in intelligence.[164] In FY2019 and FY2020, only 7% and 9% of OSIRs were used in finished intelligence, respectively.[165] OSIRs are raw intelligence reports that are supposed to be used to inform finished analytical products to answer key intelligence questions, and that is not happening with the current threat posture of CETC.

2. <u>CETC Operations</u>

a. CETC leadership provided unclear direction.

<u>Verbal commands</u>. A common refrain from employees across CETC was that leadership provided direction verbally.[166] Not all commands require a formal written memorandum, but standards, thresholds, major changes in policy, standing orders, areas of focus, and the like generally should be recorded to ensure that the direction is enduring and understandable. The

[155] Ex. A15, A43.
[156] Dissemination would be proposed by the collectors and ultimately approved by content managers/SDOs. Ex. A58. However, many collectors would pick as wide of a distribution as possible, although that practice has diminished recently. Ex. A30, A41, A50, A37.
[157] Ex. A55.
[158] The Watch is responsible for placing the OSIRs and the collected information from OSCO into eGuardian. Ex. A60. The Watch was not allowed to evaluate the threats themselves, but was told to defer to the collector's judgement and place it in the system. Ex. A4.
[159] Ex. A55, A58, A60.
[160] Ex. A58.
[161] Ex. A54.
[162] Ex. B3 (I&A OSIR Analysis Slides). SLTT and law enforcement could receive the OSIR information through eGuardian.
[163] Ex. A54.
[164] Ex. B3 (I&A OSIR Analysis Slides).
[165] *Id.*
[166] Ex. A15, A35, A39, A45, A48, A50, A60, A61, A64, A72.

CETC Director was the "king of the drive-by direction," dropping by someone's desk and asking them to do something without putting it in writing.[167] Most directions would come to the Watch verbally from the CETC Director through their Branch Manager, and if the Supervisory Team Chiefs (STCs) asked for directions in writing, they were told that verbal guidance is just as valid as written guidance.[168] The STCs responded by creating a duty log in which they tried to record the CETC Director's intent and instructions to ensure a record existed and ensure task completion occurred across shifts.[169] They would generally send this log and/or a confirmation e-mail to the CETC Director or use it to demonstrate when tasks are complete, but the Director would often say that he did not direct that task and ask, "where's the e-mail" that told them to take that action,[170] or that they had misinterpreted his instructions.[171]

Similarly, in OSCO, commands from leadership often arrived verbally.[172] Initially, the OSCO staff was also expected to verbally pass all instructions from one shift to the next.[173] Later, the collectors started using a Microsoft Teams chat log to capture what happened on each shift.[174] When employees asked for written guidance they were given excuses that leadership did not have time,[175] or that they already knew what they needed and did not need anything further in writing.[176] At best, this practice translated to wasted effort on unclear direction that changed through shift pass downs; at worst, it was construed as an attempt by leadership to have deniability for any inappropriate, accidental or intentional activities. This practice caused distrust and confusion among employees regarding task assignment and appropriateness. The desire to put leadership on the record with clear communication led some employees to take action and create their own processes, e.g., anonymous written questions and answers and minutes for the OSCO Branch Calls.[177]

Lack of standard operating procedures (SOPs). There are few written standards, SOPs, policies, tools, manuals or the like in CETC. The notable exception to this is the OSCO Cookbook, an employee written reference guide to the OSIR writing process that is outdated, incomplete and unreviewed outside of CETC.[178] The Watch has only recently started to write SOPs, with two having been approved by leadership, one of which is on the creation of CETC Notes.[179] Lacking official SOPs, employee operate by asking co-workers for guidance and direction.[180] The lack of written guidance allows gaps to persist, mistakes to multiply, provides no support to new employees in an incident, and allows institutional knowledge to leave with employees.

---

[167] Ex. A64.
[168] Ex. A55.
[169] Ex. A7.
[170] Ex. A60.
[171] Ex. A7, A4, A39.
[172] Ex. A6, A35, A37, A45, A72.
[173] Ex. A75, A61.
[174] Ex. A43.
[175] Ex. A35.
[176] Ex. A4.
[177] Ex. A37, A45.
[178] Ex. A35.
[179] Ex. A55.
[180] Ex. A6, A16, A21, A30, A32, A35, A37, A43, A41, A50 (Believing a classified collection requirement was about leaks because it was used in a previously released OSIR on a factually disparate topic and subject.), A66 A75.

b. CETC leadership and oversight support had a dysfunctional relationship.

Oversight is a critical component of the National Intelligence Program. The relationship between the intelligence components and their oversight officials and the legal office is essential to ensuring that intelligence activities are executed in compliance with applicable laws and policies. The relationship between CETC and its oversight officials (the G4 – Intelligence Oversight (IO) Office, ILD, Privacy Office (PRIV), and the Office for Civil Rights and Civil Liberties (CRCL)) was severely strained. Had it been more synergetic, the release of the questionable OSIRs may have never occurred or potentially would have been modified so that they were correctly executed. In fairness to CETC, Mr. Glawe's and Mr. Murphy's apparent animus toward oversight, especially ILD, could have been the impetus for a culture of opposition to oversight within CETC's leadership.

At the start of their new employment, CETC personnel did not receive an introduction to CRCL, ILD, the IO Office, or PRIV.[181] Many CETC employees were not even aware of the G4 as a resource.[182] One witness commented that he did not remember learning about the legal office, the role they play, or being told he could freely reach out to counsel with questions when he first joined CETC.[183] Another CETC employee asserted that he did not even know about CRCL and PRIV prior to training post-dating the Portland deployment. CETC leadership deliberately imposed barriers to impede free communication between its employees and the legal staff. Collectors were told to "follow the chain of command" before reaching outside of OSCO.[184] Although not a direct prohibition on reaching out for legal counsel, "it was hinted that it was not allowed."[185] "If you brought any knowledge from outside CETC, [leadership] would say that those outsiders do not know what CETC really does, or that the outsider didn't know what they were talking about. [The CETC Director] thought nobody knew better than him, this was especially true of the G-4."[186] An email sent by the CETC Director to CETC staff on July 17, 2020, instructed the staff as follows: "You will ensure that you utilize the chain of command for your concerns as there are often areas which you may not have the full background on why we are taking a certain action. Your supervisor or your Branch Chief will have that information and can provide you direction."[187] When a CETC supervisory team chief raised an issue about CETC's compliance with an item he identified in guidance provided by ILD, he was told by the CETC Deputy Director that the Watch should not be "second guessing the collection of the info."[188] When another junior collector first arrived at CETC, she was told that consulting legal was "not something they do at their level," instead they were instructed to talk to their superiors, and the supervisors would raise the issue with the lawyers.[189]

---

[181] Ex. A6, A14, A15, A27, A31, A32, A33, A34, A39, A45.
[182] *Id*.
[183] Ex. A32 ("I do not think we were aware of what options we had.").
[184] Ex. A45.
[185] *Id*.
[186] *Id.*
[187] Ex. B30 (Email, CETC Director to staff, subject: FW: Questions on Information Sharing in Portland, Wednesday, Nov. 18, 2020 3:04 PM).
[188] Ex. B31 (Email, CETC Director to staff, subject: RE: RO Input?, Sunday, June 24, 2018 10:20 AM).
[189] Ex. A15.

One senior leader who elaborated on the issues between the CETC Director and ILD stated that because ILD was not privy to the conversations between the CETC Director and Mr. Murphy, the extent to which Mr. Murphy provided direction to the Director might have made it so that the Director felt proscribed from going to ILD. Possibly, the CETC Director felt as if he had no authority to take ownership of the instructions directed to him because they originated from such a high level.[190]

As CETC personnel continued to raise questions and concerns surrounding the intelligence activities they were conducting, CETC leadership attempted to address the concerns in-house.[191] ILD made repeated offers to come speak with CETC employees, especially as efforts to support federal officers with the Portland civil unrest arose, but CETC leadership declined those offers.[192] ILD offered to provide further clarifying guidance on the Job Aids and legal memos it created on various topics.[193] ILD had to inject itself in CETC activities when it received notice or discovered reporting disseminated by CETC that failed to meet standards. For instance, when an ILD attorney discovered CETC was misusing the term "incite" in its OSIRs, he reached out to CETC leadership to discuss its proper use.[194] In this instance, the correction was well-received. On another occasion, ILD became concerned about "threat notifications" the Watch had disseminated on statements that fell short of a "threat" threshold. Rather than resolve ILD's concerns, the CETC Director contacted the I&A Chief of Staff (COS) to circumvent the issue. He apparently received support from the COS, as ILD was instructed to contact I&A leadership if they had concerns. ILD noted that the CETC Director routinely conducted his own legal analysis and would curtly assert "there is no issue with authority here."[195]

Threat notifications became a significant issue for CETC employees. First occurring in 2018 in response to negative public attention on certain ICE activities, CETC employees were instructed to collect and report on "any threat" against ICE personnel found in open source channels.[196] Some CETC collectors and Watch staff included memes, hyperbole, statements on political organizations, and other protected First Amendment speech in these Threat Notifications. These Threat Notifications caused such concern among collectors and watch officers that they brought their issues to CETC leadership and then to ILD. ILD provided a job aid to help CETC navigate collection on threats to ICE. The Job Aid stated

> where they [the collectors] have a reasonable belief that these activities assist the Department in identifying protective and support measures regarding threats to security, including where they have a reasonable belief that the activities would (1) constitute "true threats" to or incite violent acts against DHS personnel or property,

[190] Ex. A12, A58.
[191] Ex. B30 (Email, CETC Director to staff, subject: FW: Questions on Information Sharing in Portland, Wednesday, Nov. 18, 2020 3:04 PM).
[192] Ex. A25, 57.
[193] Ex. B32 (Email, CETC Director to staff, subject: RE Interim Supplemental Guidance on Open Source Reporting on Threatening Statements in Social Media (6), Saturday, June 23, 2018 11:30 PM).
[194] Ex. B33 (E-mail, ILD to CETC leadership, subject: RE_(U_FOUO) Daily OSIR Highlights (1 July 2020), Sunday, July 5, 2020 10:56 PM).
[195] Ex. A25.
[196] Ex. A55, A60.

> (2) provide analytically significant insights concerning an individual reasonably believed to pose a threat to DHS personnel or property, (3) in certain cases, inform an overall assessment of the risk of violence against DHS personnel or property, or (4) expose private or otherwise information about DHS personnel or facilities (i.e., doxxing), which, while not a threat per se, might result in a downstream threat of violence, including domestic terrorism, or otherwise prevent DHS from executing its lawful mission.[197]

When the CETC employees first received the ILD memo they were relieved, believing that the questionable collection they were asked to be a part of – collecting any vague threat against ICE – would no longer be allowable. However, CETC leadership told the employees that they now had their legal guidance to continue the activity unchanged and that the memo meant that all of their collection was legal and permissible under the Intelligence Oversight (IO) Guidelines.[198] This interpretation was counter to the guidance in the memorandum.[199] However, the answer by leadership was enough to discourage further dissent and created distrust between the CETC workforce and ILD. CETC leadership during this time included its Director during the Portland-related events covered in this Report, then serving as the Deputy Director.

CETC leadership was following the culture established by Mr. Murphy, who was "affirmatively hostile to ILD."[200] According to one official, whose sentiment was shared by others, "while he [Murphy] tolerated ILD and, to a much lesser extent, the other Oversight offices, he marginalized us all – sometimes with a degree of gratuitous indignation that transcended any possible merit under the circumstances and seemed at times to be more intended to influence third party observers (usually subordinates) than the ostensible targets of his hostility."[201] Mr. Murphy appeared to be displeased when the mission centers went to the G4 for review of products regarding imminent threats, likely because it delayed the release of the products.[202] In one specific instance, the Counter Terrorism Mission Center (CTMC) was adjudicating edits it had received from the oversight offices when Mr. Murphy instructed CTMC to release it, waiving the threshold concerns.[203] Similarly, the Transnational Organized Crime Mission Center (TOC) was instructed not to undergo a review process with the G4 – Mr. Murphy would ask for status updates and when someone responded that a product was under review, "he would scream that he said not to go through the G4 review process."[204] "He told the mission managers they did not have to go through G4 review, and that the G4 was there as a resource, but not a necessary step, so it was the fault of the mission managers if the review process takes time."[205] When ILD attorneys would attend I&A meetings with Mr. Murphy and the mission center

[197] Ex. B9 (Memorandum from the Intelligence Law Div. on Social Media Statements Referencing Violence Against or Doxxing of DHS Personnel and Facilities, July 13, 2018).
[198] Ex. A55, A60.
[199] Ex. A25.
[200] David Glawe appears to have had his differences with ILD leadership, but never actively discouraged engagement with ILD. In fact, he even attempted to have attorneys embedded with each mission center (a proposal that failed for lack of resourcing). Ex. A24, A33.
[201] Ex. A10.
[202] Ex. A13, A28.
[203] Ex. A13, B34 (Email, CTMC Director to ILD, subject: Requesting Immediate G4 Review for CTMC Intel Note, Thursday, June 28, 2020 9:47 AM).
[204] Ex. A29.
[205] Ex. A29, A33.

directors, Mr. Murphy would limit the attorneys' ability to provide legal guidance, making statements such as "I did not ask for your opinion."[206]

By comparison, CTMC, Homeland Identities Targeting & Exploitation Center (HITEC), and FOD have ILD integrated into their operations, in spite of Mr. Murphy's admonishments. HITEC works with ILD and IO to develop decision aids to guide their activities.[207] They collect information related to terrorism and appreciate the importance of understanding "what qualifies as a bona fide terrorism connection" and not just a loose association which cannot be used as a basis for permanent retention or dissemination of USPER information.[208] If there is any level of ambiguity, HITEC staff are instructed to engage directly with ILD and IO to determine "whether the reasonable belief standard has been met, whether dissemination is appropriate, and to whom the information can be disseminated. If either ILD or IO expresses concern, [they] yield to that and [do] not move forward until that is worked out."[209] Similarly, CTMC engages with ILD and IO on its products.[210] This is most likely because they produce finished intelligence which requires G4 review before it can be published.[211] No similar requirement for raw intelligence exists, which includes OSIRs. Despite the lack of a specific requirement, FOD, which produces raw intelligence in the form of IIRs and Field Information Reports (FIR), sent their reports to ILD for review during the civil unrest because of the potential for USPER or other civil liberty issues.[212]

c. Treatment of U.S. Person Information in OSIRs

As explained in greater detail above, DHS I&A intelligence professionals are authorized to engage in intelligence activities that further one or more of the national or departmental missions identified in the DHS I&A Oversight Guidelines. A broad range of intelligence activities furthers departmental missions, including those that support "departmental officials, officers, or elements in the execution of their lawful missions."[213] The authority of intelligence professionals to assist law enforcement is also recognized in Section 2.6 of E.O. 12333, which provides for assistance to law enforcement and broadly authorizes the IC to render assistance and cooperation to law enforcement that is not precluded by law.

OSCO's activities in Portland were undertaken to support DHS operational components, including FPS, in the execution of their responsibilities to protect against threats to people and federal buildings. The IO Guidelines permit I&A personnel to collect and retain USPI that falls within one or more categories; publicly available USPI is explicitly included as a category.

The bounds of this authority are established in the DHS I&A Oversight Guidelines, which explicitly require I&A personnel to evaluate whether USPI "would materially assist the intended

[206] Ex. A29.
[207] Ex. A49.
[208] *Id.*
[209] *Id.*
[210] Ex. A32.
[211] I&A Instruction IA-901, *Production of Finished Intelligence.*
[212] Ex. A9, A57.
[213] DHS I&A Instruction IA-1000, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (January 19, 2017).

recipient in using or understanding the disseminated intelligence of information." If not, I&A personnel "must replace it with a generic marking identifying the individual as a United States Person." If USPI is included, it must be clearly identified as such and an advisory must be included. However, the DHS I&A Oversight Guidelines explicitly state that these requirements do not apply to publicly available information."

Although the publicly available information exception to the anonymization requirement arguably allows for the dissemination of OSIRs without masking USPI, I&A historically took a more prudent course of action. The CETC Cookbook provides explicit instructions for referring to a USPER who is not the subject of an OSIR; collectors are to "redact and minimize all references to their name and use general references" such as "U.S. citizen," "U.S. person" or "U.S. company." If the OSIR is "about" a specifically named U.S. Person, the Cookbook also instructs collectors to "consider if the inclusion of USPI adds value or is relevant to the content of the report." If so, additional procedures applied.

Prior to summer, 2018, CETC's practice was to minimize USPI in OSIRs. A recipient of the OSIR could submit a Request for Information (RFI) for the anonymized USPI. If the requester articulated an appropriate need to know, the identity information would be supplied. The anonymization of USPI in OSIRs decreased the risk of civil rights and civil liberties issues with OSIRs.[214] With the understanding that USPI would be minimized, the oversight offices ceased pre-publication review of OSIRs.[215] Given the increased rate at which OSIRs were being issued, this arrangement facilitated the review process while providing for protection of USPI.

In the summer of 2018, I&A leadership sought to revisit this practice. Specifically, Mr. Murphy was interested in unmasking USPI in threat OSIRs.[216] In some situations, unmasking the USPI in a threat OSIR can make the information more actionable; identity information can be useful for a law enforcement agency that is investigating a threat.[217] In addition, the RFI process is only effective when an entity knows to ask for the information.[218] Mr. Murphy asked whether there was anything strictly unlawful about unmasking USPI in OSIRs.[219] While legal risk factors were identified and various concerns were raised, no strict legal prohibition to including publicly available USPI in OSIRs was identified.[220] Mr. Murphy decided that USPI would be unmasked in threat OSIRs.[221] This guidance was communicated to collectors.[222]

In April 2020, the Office of the Director of National Intelligence (ODNI) issued a letter titled, "Protecting the Privacy and Civil Liberties of U.S. Persons."[223] The letter described the general rule that "disseminated intelligence products should only include U.S. person identifying

[214] Ex. A2, A22.
[215] Ex. A2, A35.
[216] Ex. A46.
[217] Ex. A2, A30, A46.
[218] Ex. A46.
[219] Ex. A2, A46.
[220] *Id.*
[221] *Id.* Contrary to staff recollection, Mr. Murphy asserts Mr. Glawe made this decision.
[222] Ex. A21, A22.
[223] Ex. B2 (Memorandum, ODNI, subject: Protecting the Civil Liberties of U.S. Persons, April 29, 2020). The Under Secretary for Intelligence and Analysis was included in the distribution for the letter.

information if it is necessary, or reasonably believed to become necessary, for the recipient to understand, assess, or act on the information."

Through the letter, the Director of National Intelligence (DNI):

> direct[ed] all IC elements to review their implementation of the applicable standard for disseminating U.S. person identifying information and, as necessary, modify internal procedures to ensure the rules governing disseminations are consistently applied. Moving forward, all IC Elements should, by default, characterize U.S. person identities in disseminated intelligence reporting in a sufficiently generic manner to mask their identity, consistent with existing law and policy.[224]

The letter also requested "that each agency report back" to the memorandum within 30 days.

In response to the April 2020 ODNI letter, DHS I&A submitted a letter dated July 23, 2020 and signed by Mr. Murphy[225] that explicitly acknowledged the ODNI's direction to review "implementation of the appropriate standard for disseminating" USPI[226] and stated that DHS I&A was "especially sensitive" to the proper use of USPI. The July 2020 letter further states that "[t]his sensitivity is manifest in I&A's policies, procedures, and practices pertaining to all intelligence products, *including both raw and finished intelligence*"[227] (emphasis added) and that

I&A currently requires U.S. identities in disseminated intelligence reporting to be characterized in a manner sufficient to mask their identity. I&A's IO Guidelines require that when a USPER's identity would not "materially assist the intended recipient" it must be replaced with a generic marking prior to dissemination.[228] Analysts generally use the term "USPER" or "USBUS" (U.S. business) unless the clarity of USBUS risks disclosing an identity.[229] Nowhere in the July 23, 2020 I&A response, signed by Mr. Murphy, did I&A communicate the 2018 decision to unmask USPI in threat OSIRs or otherwise alert ODNI that I&A had made a categorical decision to unmask USPI in threat OSIRs. Significantly, collectors expressed confusion regarding the treatment of USPI in OSIRs, particularly in light of the changing guidance and lack of training on the topic.[230]

d. Quantitative Performance Metrics Encouraged a High Volume of OSIRs

OSCO collectors stated that there was a focus on the quantity of OSIRs they produced.[231] While several collectors stated that they judge themselves based on the quality of their OSIRs,[232] and

[224] *Id.*
[225] Ex. B44 (Memorandum, DHS I&A, subject: Procedures For Protecting Privacy and Civil Liberties of U.S. Persons, July 23, 2020).
[226] *Id.*
[227] *Id.*
[228] IO Guidelines, § 2.3.5.
[229] Ex. B44 (Memorandum, DHS I&A, subject: Procedures For Protecting Privacy and Civil Liberties of U.S. Persons, July 23, 2020).
[230] Ex. A30, A52.
[231] Ex. A2, A15, A26, A64.
[232] Ex. A21, A31, A34.

the Supervisory Desk Officers encourage quality,[233] collectors are judged on the number of OSIRs they publish.[234] OSCO collectors are provided with written performance metrics that identify their expected production. The expectations vary depending on the GS level of the collector. For example, to achieve excellence, a GS-9 is expected to complete three OSIRs per week[235] and GS-13 is expected to complete four OSIRs per week,[236] They are also measured by the monthly average for the year.[237] The position descriptions emphasize quantitative metrics, while providing little guidance on how to judge the quality of products.[238] Collectors were concerned that the focus on numbers resulted in some OSIRs that were not of high quality.[239]

e. The Outdated Publication Software Could Not Accommodate the Increase in OSIRs

Only two people within CETC know how to use the publishing technology, the Homeland Open Source Tool (HOST), which is archaic, cumbersome, and heavily manual.[240] This publishing software was created in-house by a CETC content manager, with the assistance of a coder, over a long weekend.[241] When it was created, OSCO had significantly fewer collectors, and the volume of OSIRs was a fraction of 2020's total.

Publishing an OSIR involves navigating three different applications.[242] The collector writes the OSIR on HOST, which is a SharePoint database. The SharePoint database connects with three databases: a reports database, an access database, and a sourcing database. The content manager has to manually input certain information into the reports database, and then the report is formatted into an email that has to be cut and pasted into a Word document. Then the content manager runs macros against the Word document to format it so that it meets IC intelligence report standards. Next the content manager uses another macro which creates two PDFs and two text documents which are put into a folder on the shared drive. Then the content manager returns to the reporting database to confirm the OSIR has been published. The content manager then sends an email to the collector so he or she can update the source database.[243]

If all processes work as intended, a very experienced content manager can complete the process in 20 minutes. The normal review and publication process varies from 20 to 90 minutes, but if technical issues exist, the process can take hours.[244]

---

[233] Ex. A22.
[234] Ex. A22, A26, A31.
[235] Ex. A27.
[236] Ex. A45.
[237] Ex. A58.
[238] Ex. A64.
[239] Ex. A15, A21, A34, A35, A45.
[240] The software was so outdated that CETC had to make a request to Microsoft to keep it supported when Microsoft was going to discontinue support to that product line. Ex. A50.
[241] Ex. A35.
[242] Ex. A22.
[243] Ex. A64.
[244] *Id.*

The steep increase in the number of collectors created huge problems with publication, and the system could not accommodate the increased volume.[245] As a result, a backlog of OSIRs developed[246] and OSIRs were becoming obsolete before they were published.[247]

Given the challenges associated with publishing OSIRs, the content managers (aka the Senior Desk Officers, SDOs) spent a great deal of their time on the technical process of publishing vice mentoring, managing, or reviewing.

During the surge associated with civil unrest, the two SDOs were working long hours without a break. One SDO reported consistently working 15-hour days without a full day off from May to July.[248] The collectors were mindful of reaching out to the SDOs because they knew how busy they were.[249]

f. Increased Focus on Publishing Threat OSIRs

I&A leadership was particularly interested in predictive intelligence and intelligence activities that would allow for the disruption of domestic events before they happened.[250] This led to efforts to identify threats in the context of events perceived to be active or in-progress.[251] Regarding open source reporting, the anecdotal successes of notifications supplied in the context of threat advisories received attention from I&A leadership and led to increased resources for CETC.[252]

At some point in the months prior to the Portland deployment, OSCO ceased its practice of assigning collectors to a particular portfolio, or subject matter area.[253] This shift was designed to move OSCO towards an "all threats," generalist approach.[254]

This move towards an all threats approach coincided with a steep increase in threats against ICE personnel.[255] CETC leadership directed its collectors to search for open source threats to law enforcement personnel, such as threats to "kill cops."[256]

Deciding whether something is a "true threat" is subjective.[257] Collectors learn to distinguish between serious threats and hyperbole through experience.[258] For example, one must consider the specificity of the threat and the context of the post at issue.[259]

---

[245] Ex. A35, A45.
[246] Ex. A35.
[247] Ex. A26, A31.
[248] Ex. A22.
[249] Ex. A26, A31.
[250] Ex. A45.
[251] Ex. A10.
[252] Ex. A19.
[253] Ex. A6, A16, A45.
[254] Ex. A45.
[255] Ex. A15.
[256] Ex. A6.
[257] Ex. A30.
[258] Ex. A27, A31.
[259] Ex. A27.

OSCO collectors began focusing their collection efforts on finding these immediate threats. The Watch would input the information into the FBI's eGuardian system and then the collector would draft an OSIR. This represented a shift in the context of duty to warn; rather than conducting searches based on varied collection requirements and fulfilling their duty to warn when they identified threat information incidental to their searches on other topics, the OSCO collectors specifically searched for threats that could give rise to a duty to warn.

The increased focus on threat OSIRs had three unanticipated consequences. First, collectors, particularly new collectors, became less familiar with collection requirements because they were focusing most of their attention in one discrete area, and used the same two collection requirements for the bulk of their OSIRs. Second, the urgency with which threat OSIRs have to be published led to a constant expectation of immediate action. Third, given that the vast majority of OSIRs written were threat OSIRs, the decision to unmask USPI in threat OSIRs meant that the collectors were becoming accustomed to seeing USPI in OSIRs and were not as accustomed to ensuring appropriate anonymization.

g. OSIR Review Process

A collector is responsible for sending the draft through the OSIR review process. Before Portland, the pre-publication process for reviewing OSIRs consisted of a peer review, and then review by the content manager.

An essential part of the OSIR review process is ensuring that the OSIR fulfills an intelligence need identified by a collection requirement. There are Priority Intelligence Requirements (PIRs), Essential Elements of Information (EEIs), and Standing Information Needs (SINS), among others.[260] Draft requirements articulate intelligence gaps (needs), are properly validated, are coordinated with IC members and the DHS IE, and undergo thorough oversight review prior to publication in the appropriate systems.[261] Requirements are created to address analytical needs, customer needs, and CINT priorities. OSCO collectors should engage in collection of information to meet assigned OSCO collection requirements. Collection practices, including the use of search terms, should be designed to collect information that fulfills an intelligence need identified by a collection requirement. An appropriate review process should identify a draft OSIR that is not responsive to a collection requirement, and the draft OSIR should be held pending resolution of that issue.

Given the training issues, newer collectors learned how to write OSIRs, in part, by looking at previously published OSIRs.[262] Consequently, collectors learned to view published OSIRs for reference. Collectors used this practice to identify an applicable requirement; they viewed previous reporting on similar subjects when they went about the process of identifying the applicable requirement.[263]

[260] Ex. A45.
[261] Ex. A40.
[262] Ex. A15, A26.
[263] Ex. A31.

Some collectors stated that some collection requirements are unclear or general. At times, identifying the correct collection requirement can be challenging. Sometimes collectors identified information that did not fit neatly within a collection requirement, so they identified the requirement that fit best.[264]

Due to the increased focus on publishing threat OSIRs, by May 2020, the new collectors were only looking for threats of violence or incitement of violence relating to the civil unrest. As a result, some of the new collectors were only familiar with two of the collection requirements, specifically, the ones on direct threats and threats of violence.[265]

The quality of peer review varied. Moreover, not every collector made changes based on peer review.[266]

The collectors in Portland were particularly junior and inexperienced. While they were in Portland, their communication was limited with their colleagues in Washington, DC, particularly because of the time zone difference and hours worked. As such, they conducted peer review for one another. They were also working long hours, and some stated that they were so busy it was hard to think beyond the day to day work.[267]

### B. The Deployment of I&A Personnel to Portland was Poorly Planned and Executed

I&A faced significant challenges that impaired its execution of the deployment to Portland. Leading up to the events in Portland, I&A had begun placing greater emphasis on supporting law enforcement operations.[268] Consistent with this expanded vision of I&A's role and mission, through personnel situated across the nation in FOD, I&A provided direct support on several active shooter incidents in 2019. Typically, FOD personnel would deploy to a command post near an incident or a planned special event, which would enable FOD to exchange information with law enforcement officers on the ground and enable the FOD employee to provide I&A leadership with general situational awareness.[269] Prior to 2019, FOD also provided support to sheriff's offices and other law enforcement agencies during the southwest border surge.[270] According to FOD's Deputy Director (East), he had personally been responsible for planning and executing I&A FOD's SW border surge.[271]

On those prior occasions when FOD deployed its personnel, OSCO did not similarly send its collectors to the affected locale.[272] During events and crises, such as the 2018 midterm elections and the active shooter incidents in El Paso, TX, OSCO surged collection efforts, but continued to perform its mission from within the National Capital Region (NCR).[273]

---

[264] Ex. A21.
[265] Ex. A52.
[266] Ex. A27.
[267] Ex. A52.
[268] Ex. A9, A54.
[269] Ex. A9, A17, A56.
[270] Ex. A9, A28.
[271] Ex. A9.
[272] Ex. A18.
[273] Ex. A45. A50.

This recent experience of FOD deploying additional personnel to specific locales, while OSCO could expand its own efforts in the NCR, was the operational backdrop in place when the May 25, 2020 George Floyd killing triggered an extended period of civil unrest affecting the entire country. As the place where Mr. Floyd was killed, Minneapolis was one of the first flashpoints. In response, to help cover the events unfolding in Minneapolis, FOD assigned an Intelligence Officer based in (b) (7)(C), (b) (6) to assist with those efforts from her remote station; this (b) (7)(C), (b) (6) -based Intelligence Officer later spent a significant amount of time on the ground in Portland.[274]

In the following days, it became apparent that civil disturbances would not be confined to Minneapolis; other cities around the country were impacted as well. Indeed, on the night of May 29, one FPS security officer was killed and another one was injured in Oakland, CA amid protests occurring there.[275] Coincident with the shootings of the FPS officers in Oakland, CA, Portland experienced its first "riot" on May 29.[276]

1. I&A's activities were impaired from the outset by its lack of a presence in Oregon prior to George Floyd's killing.

Immediately after the shootings of the FPS officers in Oakland and the Portland riot, I&A leadership directed that FOD intensify its collective efforts to support law enforcement agencies on the ground wherever civil unrest was occurring, which by this point numbered more than 20 cities.[277] With respect to Portland, however, FOD recognized a potential gap coverage because Portland had not had an intelligence officer stationed in Oregon for about two years.[278] FOD had been covering Portland remotely utilizing staff from other states. Remote coverage, however, did not offer the best opportunity for FOD to build and maintain relationships with officials associated with the Federal, state, and local law enforcement agencies responding to the situation in Portland. Had there been a full-time FOD official based in Oregon at this time, he or she would likely have already been in direct and consistent communication with partner agencies at the Oregon fusion center located in Salem, OR.[279] Without the ability to obtain information directly from familiar law enforcement officials responding to the evolving situation in Portland, FOD was at a disadvantage in its ability to provide accurate, credible, and timely situational awareness information to I&A leadership, including Acting USIA Murphy.[280]

To try to begin filling this identified gap, and consistent with Acting USIA Murphy's reported urging that FOD not only perform its traditional situational awareness role, but to also "get ahead of events,"[281] on May 30, 2020, FOD deployed one of its out-of-state officers from within FOD's

[274] Ex. A18.
[275] Ex. A67, B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)); "Federal Protective Service officer killed, another injured in Oakland shooting amid George Floyd protests," *NBC News* (May 30, 2020), https://www.nbcnews.com/news/us-news/federal-protective-service-officer-killed-another-injured-oakland-shooting-amid-n1219561.
[276] Ex. A69.
[277] Ex. A67, B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).
[278] Ex. A9, A18, A56.
[279] Ex. A56.
[280] Ex. A56, A69.
[281] Ex. B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).

Pacific Northwest region to the Salem, OR fusion center. The FOD officer who travelled to Salem, OR did so during a weekend when the fusion center was closed. Thus, he had to work out of a hotel and did not meet anyone in person. The FOD officer made a number of phone calls from his hotel room, and he returned to his home base (b) (6), (b) (7)(C) at the end of the weekend. [282] It is not clear how successful this trip was in terms of FOD's hopes to strengthen ties with law enforcement agencies operating in Oregon for what would lie ahead.

In the following days, violence and civil disturbance in Portland continued unabated. After the conclusion of the first FOD officer's trip to Salem, OR, FOD continued to cover the situation in Portland remotely through staff based in other states. From the vantage point of the Director of FOD and the Regional Director for the Pacific Northwest Region (which includes Oregon), the violence in Portland grew worse and appeared more sustained and intense as compared to other American cities.[283] Around June 15, under continuing pressure from I&A headquarters to provide support with respect to the violence in Portland, FOD/Pacific NW sent a volunteer staff member to Portland. Joining the analyst in Portland was another volunteer, an intelligence officer based in (b) (7)(C), (b) (6), within FOD's Rocky Mountain Region. Both individuals worked in Portland from June 16-23, staying at a hotel near Portland's airport. Neither of the FOD staff members deployed to Portland during this period worked at the FPS command center in downtown Portland, located in the immediate vicinity where violence and civil disturbance were occurring.[284]

While the two FOD staffers were in Portland, they sought to build relationships from the ground up. The relationships had apparently withered in the absence of a full-time staff dedicated to and located in Oregon. They met and connected with officials from various agencies, including FPS, the U.S. Marshals Service, and FBI throughout the week, while also monitoring events on the ground as they occurred after sundown. After laying the groundwork for better interagency relationships, the two FOD staffers left Portland on June 23.[285] The intelligence officer based in (b) (7)(C), (b) (6) told the I&A review team that she was not expecting to come back to Portland when she left that day.[286]

2. Brian Murphy Directs the Deployment of FOD and OSCO Personnel on July 8 despite the lack of Adequate Planning and Preparation for Deployment.

Following the departure of the FOD staffers from Portland, the city continued to experience extensive, unabated violence. As the July 4th holiday approached, FOD recognized there could be an increase in violence and nefarious activity that could threaten federal employees and facilities. To plan for the anticipated threat, FOD compiled a Field Operations Posture manual to identify FOD's available resources and potential gaps in coverage throughout the nation during the July 4th weekend.[287] This document was developed to help guide FOD's reaction in the event that resources had to be re-deployed to address a trouble spot.

[282] Ex. A69, B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).
[283] Ex. A67, A69.
[284] Ex. A11, A18.
[285] *Id.*
[286] Ex. A18.
[287] Ex. B15 (*Department of Homeland Security Field Operations Operating Posture July 4, 2020* (June 30, 2020)).

The July 4th weekend passed without issues relevant for this report. Soon thereafter, however, without anticipation and prior deliberation with FOD and CETC,[288] Senior Official Performing the Duties of the Principal Deputy Under Secretary for I&A (SOPDPDUSIA) Jen, at the direction of Acting USIA Murphy, instructed both FOD and CETC to deploy personnel on the ground to Portland to support law enforcement partners there.[289] Although this directive was communicated by SOPDPDUSIA Jen, the universal consensus among the witnesses was that he was doing so at the behest of Acting USIA Murphy.[290] Indeed, Mr. Murphy confirmed during his interview with the I&A review team that he directed FOD and OSCO to deploy into Portland.[291] This directive was issued, however, without a codified plan of action describing how such an operation could be executed successfully.[292] Unlike the previous SW border surge, there was no planning for Portland.[293] There was also no experience or precedent for deploying OSCO collectors to a location where violent events were occurring.

The lack of planning for the Portland deployment was evident from several complications that CETC and FOD soon realized and had to overcome. First, the I&A footprint that Acting USIA Murphy and SOPDPDUSIA Jen initially directed to be deployed to Portland was large, consisting of eight I&A personnel. As specific individuals were identified for deployment, however, no plan (or even realization) existed for where exactly the individuals would work. Consequently, shortly after the arrival of the OSCO team in Portland, FOD's intelligence officer from (b) (7)(C), (b) (6), who was asked to go to Portland for a second time, had to make impromptu arrangements to find appropriate workspace for the OSCO team. She ultimately succeeded in negotiating sufficient space to accommodate the OSCO team at a Portland Police Bureau training center located near Portland's airport.[294] Finding this space was fortuitous because it served to diminish, for the time being, the OSCO collectors' potential exposure to danger at the downtown Portland epicenter.

Another complication that I&A had to overcome in getting its collectors to Portland involved the fact that the OSCO collectors had not yet been issued travel cards.[295] In all likelihood, there probably had not been a perceived need to issue travel cards to junior OSCO employees because there had not been a preexisting expectation or precedent for them to deploy to any sort of operating environment, let alone a chaotic one. The need to issue travel cards to them was also probably not recognized beforehand considering that some of the OSCO collectors had

[288] Indeed, the only noteworthy consultation that occurred was interagency discussion between I&A leadership and FPS leadership, during which SOPDPDUSIA Jen notified his counterpart at FPS that I&A would not be able to provide HUMINT collection or perform undercover work. Ex. B17, Email "10_Email - (U__LES) DHS Rapid Deployment Team (RDT) CONFERENCE CALL_ 1300 ET Wednesday 8 July 2020 (002)."
[289] Ex. B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).
[290] Ex. A56, A58, A67.
[291] Ex. A46.
[292] FOD appeared to have quickly compiled a two-page paper on its deployment entitled *PORTLAND SURGE OPERATION", CONOPS, CIVIL UNREST – THREATS TO LAW ENFORCEMENT/FEDERAL FACILITIES, 8-15 July 2020.* Ex. B17 (Attachment to Email "10_Email - (U__LES) DHS Rapid Deployment Team (RDT) CONFERENCE CALL_ 1300 ET Wednesday 8 July 2020 (002))."
[292] Ex. B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).
[293] Ex. A9, A56.
[294] Ex. A18.
[295] Ex. A43, A50.

onboarded during or shortly before the onset of the COVID pandemic, during which time travel was generally not encouraged. The mundane issue of ensuring that the collectors could easily pay for their expenses while on temporary duty had to be resolved in a rapid fashion.

The lack of planning for the Portland deployment also resulted in inadequate consideration for the personal safety of the individuals situated near the violence happening on a nightly basis in Portland. According to FOD's intelligence officer from (b) (7)(C), (b) (6) who deployed to Portland, the threat on the ground was quite real. She assessed the counter-surveillance activities in Portland to be troubling and threatening to law enforcement.[296] This assessment is consistent with the descriptions provided by three of the OSCO collectors in Portland, who said that the locations of the hotels where DHS personnel were lodging during the deployment had been compromised, including the hotel at which the OSCO collectors were staying.[297] The FOD Director also received reports of FOD personnel being followed in their rental vehicles, which necessitated changing cars.[298]

In speaking with the FOD personnel who deployed to Portland, the general consensus was that while this operating environment was quite stressful, they did not personally feel unsafe and could manage the situation. This view is understandable given that the FOD personnel who deployed were seasoned professionals, many of whom had prior careers in law enforcement or the military.[299] In contrast, the OSCO collectors were relatively young and lacked military or law enforcement experience.[300] Prior to going to Portland, the OSCO collectors were given a CI briefing to help them acclimate to the operating environment into which they were entering.[301] The CI briefing did have one concrete benefit, which was that the collectors returned home to repack their clothing – they had packed business attire, which would have made the group stand out in the operating environment.[302] It is unclear, however, how a short CI brief could prepare the OSCO collectors mentally for the conditions they would face.

In addition, the OSCO personnel who deployed lacked sufficient equipment and training to overcome physical threats to their health and safety. In Portland, tear gas was employed by law enforcement in efforts to contain violent activity. However, violent opportunists had also conceived tactics to counter-fire the tear gas canisters.[303] Potential exposure to tear gas was a significant concern after the OSCO collectors were forced out of their work space at the Portland Police Bureau training facility near the airport due to the passage of a Portland City Council resolution directing the Bureau to no longer coordinate efforts with Federal agencies.[304] The passage of this resolution forced the OSCO collectors to move their center of operations to the Edith Green Building, near the protest and related violent activity. This building's ventilation

[296] Ex. A18.
[297] Ex. A30, A52, A72.
[298] Ex. A67.
[299] Ex. A17, A18, A56, A69.
[300] Ex. A43, A52, A58.
[301] Ex. A19, A30, A43, A52, B27 (Email, OSCO Director to staff, subject: Meeting at 1300 at the NAC, July 9, 2020 1026 AM).
[302] Ex. A43, A52.
[303] Ex. A70.
[304] Ex. B18 (Email, OCSO Director to CETC Director, subject: Re Portland City Council Resolution, July 22, 2020 9:18 PM).

system was flawed, however, and sucked tear gas used outside inside.[305] Exposure to tear gas was also possible when I&A employees were entering and leaving the vicinity.

Prior to the forced move of OSCO collectors, only FOD personnel were situated near the violent activity. For a time, however, the FOD personnel could not protect themselves from tear gas because they did not have gas masks.[306] Although many of the FOD personnel on the ground had the proper training to use gas masks from their prior experiences, this training was no help without having the equipment. The OSCO team that deployed had the opposite problem – they were issued gas masks at a meeting at the DHS Nebraska Avenue Complex (NAC), but had limited knowledge on how to use the masks. Upon being given the masks at the NAC deployment orientation, OSCO's Branch Chief and FOD's Deputy Director (East) conducted a session to train the OSCO personnel on how one should use a gas mask. The trainers were able to offer this instruction not from any training they received at I&A, but rather from experiences from their prior careers.[307] After the OSCO team arrived in Portland, the collectors also received guidance on how to use a gas mask from the FOD team lead deployed from (b) (7)(C), (b) (6).[308]

I&A personnel were also initially not prepared to protect their eyes from laser beams pointed at them by violent opportunists. This was a significant concern for personnel entering and exiting the command center, due to the point of ingress and egress being a choke point. Laser pointers pose a significant threat because eye exposure could result in permanent damage to one's vision. To address this threat, personnel entering and exiting the command center building had to wear a special pair of eyeglasses that are designed to protect one's eyes from lasers.[309]

FOD sought assistance from I&A headquarters to obtain safety equipment quickly, but found that the procurement processes were not nimble enough to get them what they needed immediately. Ultimately, FOD was able to obtain laser-shielding eye glasses from FPS after requesting their assistance.[310]

From July 23-27, FOD's Deputy Director East personally made a trip to Portland to observe the situation first-hand in order to assess whether personal safety issues were being addressed adequately. Despite the legitimate concerns over the personal safety of I&A's personnel during the earlier stages of the deployment, the Deputy Director judged that the equipment and procedures for ensuring the safety of I&A's workforce had become adequate by the time of his observation and therefore I&A personnel need not be withdrawn for safety reasons.[311]

3. <u>OSCO's Volunteers for the Portland Deployment Lacked Experience, Training, and Equipment on Open Source Collection.</u>

[305] Ex. A56.
[306] Ex. A18, A56.
[307] Ex. A56.
[308] Ex. A18.
[309] *Id.*
[310] *Id.*
[311] Ex. A56.

Starting in June, OSCO surged its open source collection efforts in response to the civil unrest, to include events happening not just in Portland but in other cities around the country.[312] The idea for I&A to surge may have originated from a request made by FPS on May 30 for I&A to provide OSCO support following the death of an FPS officer the previous night.[313] OSCO's work on covering the national unrest beginning in June was performed in the NCR by collectors working from home.[314] The emphasis of OSCO's efforts began to shift specifically onto Portland on June 12, 2020, when CETC's Director emailed his organization to initiate a full court press on Portland and two other cities.[315] During this first surge, OSCO's staff was asked to work extra hours; one of OSCO's SDOs said she continually worked 15-hour days during this period.[316]

When the first surge commenced, however, many of OSCO's collectors who had recently on-boarded, had not yet worked on open source collection, even though they may have already been with the organization for two or three months. The newly hired collectors could not collect because they did not have specialized laptop computers to enable them to conduct their research in an appropriate manner.[317] To comply with the instruction to surge, OSCO leadership had to obtain laptops and distribute them quickly. According to OSCO's Branch Chief, I&A personnel from within I&A Intelligence Enterprise Resources went to several retail outlets to purchase laptops using P-Cards.[318] Once obtained, the laptops were distributed during a Saturday night meeting at the NAC.[319] Only then did the recent hires begin working on open source collection. Thus, when OSCO was directed on July 8 by SOPDPDUSIA Jen (at the behest of Acting USIA Murphy) to deploy collectors into Portland, OSCO had to potentially draw from a workforce consisting of many collectors who had only about a month of OSCO open source collection experience.[320]

When OSCO was directed to deploy, it worked to identify its Portland team by first soliciting volunteers for the mission through an email sent by OSCO's Branch Chief at 1:22pm on July

[312] Ex. A50.
[313] Ex. B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).
[314] Ex. A45.
[315] Ex. B47 (Email, OSCO Director to CETC Director, subject: "RE **HOT**, June 12, 2020 9:36). The June 12, 2020 email appears to have been motivated by a 9:00am leadership meeting at which FOD's Director records Acting USIA Murphy as having said "start writing on what we see!" Ex. B14 ("Over notes" (FOD Director's notes made in preparation for his appearance before HPSCI)).
[316] Ex. A22.
[317] Ex. A43, A45, A52.
[318] Ex. A50.
[319] Ex. A43, A50, A52.
[320] The Director of OSCO recalls a similar sequence of events occurring but implied that the acquisition and distribution of laptops occurred on July 9, 2020, at the same time when the OSCO team members who had been selected to go to Portland gathered to receive gas mask training and a CI briefing. The Director of CETC complained about OSCO not having a stockpile of laptops and instead having to rely on the readiness side of I&A to utilize P-cards to purchase laptops on an as-needed basis. Ex. A58. However, his description of the timing of the sudden purchase and distribution of laptops as having occurred to allow OSCO's Portland deployment team to be properly equipped with open source collection equipment is doubtful because the OSCO collectors being sent to Portland had their own laptops by then. Ex. A43, A52, A72. The CETC Director's recollection on this issue is plausible only if OSCO's Portland deployment team needed backups or substitute devices that were durable enough to withstand the tough operating environment.

8.[321] Positive responses mostly came from a younger cadre of collectors who had on-boarded with OSCO in late 2019 or early 2020.[322] During interviews, CETC's Director noted that it was understandable that more senior collectors did not volunteer due to the likelihood that they had family and other commitments.[323] When one of the slightly more experienced OSCO collectors who volunteered but was not selected to go to Portland later learned that it was "all new people" going to Portland, he thought that this was not a wise move on management's part and that it would set the organization up for failure.[324]

OSCO was directed to send five individuals to Portland. The initial five-person team that the CETC Director and the OSCO Branch Chief sent consisted of the following:

- Collector #1: This individual on-boarded with OSCO on January 20, 2020. Throughout the relevant period, (b) (7)(C), (b) (6) . Prior to coming to OSCO, (b) (7)(C), (b) (6) However, those positions involved analysis, not collection. Collector #1 received and reviewed materials that were given to her, including the OSCO Cookbook, but did not receive any formal I&A training prior to being sent to Portland. She did receive on-the-job training with fellow collectors in the first six weeks during which she was employed by OSCO.[325]
- Collector #2: This individual, who has since transitioned to a different mission center, was first assigned to OSCO as an open source collector on May 11, 2020. Prior to that, Collector #2 worked for I&A as an (b) (7)(C), (b) (6) . When he was deployed to Portland, (b) (7)(C), (b) (6) . When undergoing placement (b) (7)(C), (b) (6) Collector #2 ranked three options: HITEC, Counterintelligence Mission Center (CIMC), and CETC. Collector #2 was placed in CETC despite that being his third choice. Collector #2 did not have much work to do during his first few weeks at CETC. Aside from receiving the Cookbook and other emails, he was not given guidance on what to collect before he began collecting.[326]
- Collector #3: This individual began working for OSCO in April 2020. Prior to that, she worked (b) (7)(C), (b) (6) . In April and May, Collector #2 conducted some training on a distance basis but not through a formalized training procedure. She apparently first received equipment necessary for open source collection in May and was told to begin collection without further instructions or guidance on how to perform that work. She was told to obtain further guidance from more senior OSCO personnel.[327]
- Collector #4: This individual on-boarded as an OSCO open source collector in May 2020 (b) (7)(C), (b) (6) . Prior to that, (b) (7)(C), (b) (6) Collector #4 did not have any formal training until he took an OSINT 101

[321]Ex. B19 (Email OSCO's Branch Chief to OSCO distribution list, subject: RE NEW REQUEST FOR TRAVEL," July 8, 2020 1:48 PM).
[322] Ex. A16, A37, A58, A69.
[323] Ex. A58.
[324] Ex. A16.
[325] Ex. A72.
[326] Ex. A52.
[327] Ex. A43.

course at ITA about a month before the investigation team spoke with him. This collector also had not yet participated any further CETC training. He was essentially told in May to review the Cookbook and if he had questions, he should ask a senior collector. Collector #4 ultimately stayed in Portland for about a week to 10 days.[328]

- Collector #5: Although the investigation team did not record when collector #5 on-boarded with OSCO, she seems to have begun working for OSCO sometime after the onset of COVID. Collector #5 said she had undergone generic trainings through PALMS and taken a McAfee training during her initial time at OSCO. She also recalled receiving and reading the Cookbook. However, she did not have an opportunity to shadow anyone due to the COVID operating environment.[329]

Although the Director of CETC immediately noticed the volunteers selected for deployment were young and inexperienced, it is unclear the extent to which this specific concern was effectively communicated to Acting USIA Murphy and Mr. Jen, then Senior Official Performing the Duties of the Under Secretary of I&A (SOPDUSIA), following Mr. Murphy's appointment as Acting USIA in May 2020. Earlier in the day, prior to the Branch Chief's solicitation for volunteers, the CETC Director and the OSCO Branch Chief both pushed back against the instruction to send an OSCO team to Portland.[330] However, their concerns may have focused on the lack of need to send individuals to Portland to perform open source collection, since open source collection can be performed any place with an internet connection.[331] The COVID pandemic may also have been offered as a reason for not wanting to deploy OSCO to Portland.[332] However, no one with whom the review team spoke could definitively recall whether CETC identified training deficiencies with its workforce as a reason for why they should not be deployed.[333]

Whatever the substance of the objections raised to the I&A front office, CETC did not persuade the front office to reconsider the decision to deploy OSCO personnel to Portland. Following the solicitation for volunteers, CETC's leadership apparently viewed the decision as one that had been made and could not be reversed.[334] No further efforts were made by CETC's leadership to persuade I&A's front office to modify the decision to deploy OSCO to Portland. CETC's leadership apparently did not communicate to the I&A front office CETC's concerns with the capabilities of the OSCO team being sent to Portland after the team members' potential shortcomings became plainly evident.

Initially, there were no plans for the Branch Chief to go to Portland with the OSCO team of collectors. CETC's leadership recognized, however, that it would be unwise to send the inexperienced and untrained collectors to Portland on their own. CETC's leadership may have explored the possibility of leveraging the presence of senior FOD personnel to supervise OSCO collectors. CETC's leadership ultimately did not feel comfortable with its open source collection

[328] Ex. A62.
[329] Ex. A30.
[330] Ex. A50, A58.
[331] Ex. A28, A58.
[332] Ex. A58.
[333] Ex. A12, A28, A46.
[334] Ex. A50, A58.

work being overseen by field employees who lacked insight into how open source collection is performed.[335] Accordingly, the Director of CETC agreed with the OSCO Branch Chief that she should accompany the collectors to provide leadership.[336] While the decision to have the Branch Chief accompany the junior collectors may have been the best, and perhaps the only realistic, solution available under the circumstances, it was not ideal. The OSCO Branch Chief appeared outwardly to be a logical choice by mere dint of her position.[337] However, despite extensive experience within the intelligence community across the Federal government, the Branch Chief had only begun working at I&A in August 2019.[338] Furthermore, she had never been an open source collector and may not have been fully versed on the tradecraft and requirements involved in open source collection.

OSCO's deployment to Portland lasted from July 9 – August 4, but the above identified collectors did not stay in Portland the whole time. Collectors #4 and #5 only stayed in Portland for 7 - 10 days. Collector #2 had to be back in DC on July 20-21. During the latter part of the deployment period, OSCO identified a need to backfill for one of the collectors who had returned to the NCR and did not come back. Accordingly, OSCO's Branch Chief sent out an additional solicitation for volunteers, which led to a 6th collector being chosen to go to Portland:[339]

- Collector #6: This individual on-boarded with OSCO in March 2020 (b) (7)(C), (b) (6). Prior to that, (b) (7)(C), (b) (6). Collector #6 indicated to the investigation team that due to Covid-19, the collectors were told to start collecting and that they would be trained later. Collector #6 took many of the available online trainings through DHS PALMS and other free trainings such as one provided by McAfee. Collector #6 was also given the Cookbook and told to read it. He did not have formal training until after the Portland deployment.[340]

CETC was still unable to identify an experienced collector who would be willing and able to go to Portland.[341]

4. I&A Failed to Establish and Implement a Clear Command Structure to Oversee and Support its Deployment to Portland.

In addition to issuing the orders for FOD and OSCO to surge an on-the-ground presence into Portland on July 8, SOPDPDUSIA Jen was also nominally placed in charge of leading the execution of the deployment. Mr. Murphy now asserts that he placed Mr. Jen in this position in order to "unify command" between the two sides of I&A – DUSIER and DUSIEO, while he personally only engaged in general oversight.[342] Mr. Jen confirms that Acting USIA Murphy

[335] Ex. A58.
[336] Ex. A58, B42 (Email, OSCO Director to OSCO staff, "Deployment to Portland," July 9, 2020 7:23 AM).
[337] Ex. A12.
[338] Ex. A50.
[339] Ex. B21 (Email, OSCO Director to OSCO staff, subject: Request for Additional Collectors in Portland, July 25, 2020 10:44 PM).
[340] Ex. A6.
[341] One of the more senior collectors may have been willing to go at this time to Portland but for medical reasons was not a good option. Ex. A45, A50.
[342] Ex. A46.

wanted him to "honcho" on the Portland effort.[343] According to the Acting DUSIEO during the deployment, she had asked that SOPDPDUSIA Jen be put in charge of the deployment because of her fairly recent appointment to the position (May 2020), comparatively short tenure at I&A, and unfamiliarity with CETC. The Acting DUSIEO also asserted that while she was copied for awareness on emails relating to the handling of the deployment, she was not part of the decision-making process.[344] The extent of her dissociation with matters relating to the deployment, however, is somewhat disputed by Mr. Jen, who said that the Acting DUSIEO "was part of the decisions we were making."[345]

Whichever leader was responsible for unity of command, one issue that was never resolved was the bifurcation of roles and responsibilities between CETC and FOD as they operated side-by-side in Portland. With the decision to also deploy OSCO's Branch Chief to Portland, there were two senior leaders for each of OSCO and FOD present. According to Mr. Murphy, by policy, unity of command should have been conducted through FOD, although SOPDPDUSIA Jen "could have waived that if he wanted to … organize it differently."[346] According to the Director of FOD, he shared his concerns over the bifurcated chain of command between OSCO and FOD with SOPDPDUSIA Jen. The FOD Director's position on this matter is consistent with the views uniformly expressed by his subordinates,[347] although this issue was only mentioned as potentially problematic by one neutral observer.[348]

In response to the issue of bifurcation of command raised by the FOD Director, it is not clear whether SOPDPDUSIA Jen truly sought to resolve the issue one way or the other. Apparently, the FOD Director seemed resigned to the fact this was the type of issue on which SOPDPDUSIA Jen would not get involved.[349] The Director of FOD then raised the issue directly with the Director of CETC and the then-DUSIEO, but the matter was never resolved to the FOD Director's satisfaction.[350] According to CETC's Director, he had conversations on this matter with FOD's Deputy Director (West), in which he politely pushed back on the notion that FOD should be put in charge of the entire Portland operation. CETC's Director told the investigation team that he perceived FOD's Regional Director for the Pacific Northwest as having ulterior motives for pursuing consolidation of the chain of command within FOD.[351]

Operationally, on issues relating to open source collection and production of OSIRs, OSCO was solely responsible and FOD had no role. OSCO and FOD did cooperate to a limited extent on the distribution of Operational Background Reports (OBRs) – during the period when OSCO and FOD were not co-located, OSCO had to transmit their completed OBRs to FOD, who then shared the products with FPS.[352] OSCO subsequently provided OBRs directly to FPS.[353]

---

[343] Ex. A28.
[344] Ex. A12.
[345] Ex. A28.
[346] Ex. A46.
[347] Ex. A9, A17, A18, A56, A69.
[348] Ex. A54.
[349] Ex. A54.
[350] Ex. A67.
[351] Ex. A58.
[352] Ex. A18.
[353] *Id.*

Meanwhile FOD continued to play its traditional role of obtaining and passing on relevant information to its co-located partners. In addition, FOD led efforts to ensure that all I&A employees in Portland could work safely. However, FOD's leading role on ensuring that no one put him or herself in danger was apparently not always recognized in practice. According to FOD's Regional Director (Pacific Northwest) , OSCO did not communicate effectively with her on its activities.[354] Both FOD's Director and Deputy Director (West) identified an incident in which OSCO ignored FOD's advice to not work at a particular location due to safety concerns for one specific night.[355] The FOD team lead from (b) (7)(C), (b) (6) also felt that her judgments regarding personal safety were considered "advisory" as opposed to "authoritative," with the advice sometimes being set aside if the recipient either did not realize the risk or had a higher risk tolerance.[356] An email circulated within FOD indicates that OSCO appeared to have disregarded FOD's safety-related recommendations on more than one occasion.[357]

Within OSCO itself, there were questions as to its own command structure during the end of its deployment to Portland, when the OSCO Branch Chief departed the scene on July 28, 2020. From then until the rest of the OSCO collectors returned to the National Capital Region (NCR) on August 4, 2020, Collector #1 was in charge of OSCO's efforts in Portland. Collector #1 was only a GS-7 employee, although she somehow had the most experience among the collectors left in Portland.[358]

As explained by OSCO's Branch Chief, she did not perceive her early departure to be problematic. She complimented Collector #1 on her capabilities and her ability to work with CETC's partners. In addition, the Branch Chief continued to check with the collectors still in Portland twice per day. [359]

CETC's Director also did not regard his Branch Chief's early departure to be problematic because he thought that the Branch Chief left only two days before the rest of the OSCO team left. He said that by the time the OSCO Branch Chief was leaving, it was apparent that OSCO's presence was already winding down and that the collectors were "on a glide path to come home."

The CETC Director's explanation of the timing cannot be accepted, however, in light of his own Branch Chief's assertions that she left on July 27/28, at which time OSCO's work was not yet winding down. On that date, the OSIRs themselves had not yet been leaked to the press, and Acting USIA Murphy had not yet been detailed out of I&A. The OSCO Branch Chief's recollection of her departure date being July 28 is also corroborated by the account of a CTMC analyst as having deployed to Portland on July 28, on the same day that the OSCO Branch Chief left. This analyst also recounts the OSCO team being present for the 7-8 days during which he was in Portland.

---

[354] Ex. A69.
[355] Ex. A9, A67.
[356] Ex. A67
[357] Ex. B20 (Email, FOD RD to FOD senior headquarters leadership, subject: Health and Safety Issues and Questions," July 23, 2020 4:15 PM).
[358] Ex. A6, A43, A52, A72.
[359] Ex. A50.

The OSCO Branch Chief's early absence from Portland was a significant concern of the Regional Director deployed to Portland at the time. This Regional Director already had concerns about the OSCO personnel being "kids" and felt that leaving a GS-7 employee to oversee OSCO operations in Portland was not a good idea. The Regional Director's concerns motivated him to write an email addressed to the CETC Director, in which he is urged to delay the OSCO Branch Chief's departure for several more days to help with integrating the OSCO team with his own. In response, the CETC Director insisted that the OSCO Branch Chief had to come back due to "the compelling need to have her back her[sic] managing her branch in other areas that reach beyond Portland takes precedence at this point in time."[360]

The email sent by the Portland Regional Director also alludes to another issue impacting the structure and organization of the deployment at the time – he refers to "our footprint is also growing over the next couple of days, that combined with some of your folks coming out too…." The Regional Director was referencing the plans for additional FOD personnel to deploy to Portland from around the country, consistent with the direction originally given by Acting USIA Murphy on July 8. By the time of this Regional Director's deployment to Portland, other headquarters personnel from other mission centers were being deployed to Portland. As noted above, an analyst from CTMC arrived in Portland on July 28. The RD also recalls someone from CIMC and three others from the Collections Management Division came to Portland.[361]

The Regional Director for Portland did not feel that the addition of these individuals would be useful, and he complained to FOD Deputy Director (West). When the extra staff arrived anyway, the RD did not find the extra bodies to be truly useful. The Regional Director found the presence of the personnel from the Collection Management Division to be especially not helpful because they seemed to have been sent by headquarters without a true understanding of the practical limitations on the collectors' ability to gain useful information.[362] Similarly, the Director of CIMC said she contributed one of her staff to go to Portland at this time. The CIMC staffer apparently was in Portland for only two days, during which he was apparently told that there was not anything for him to do.[363]

The questionable usefulness of the extra people being sent at this time is demonstrated by the unclear purpose for deploying the CTMC analyst to Portland. This individual had only recently become an analyst assigned to the Travel and Immigration Branch, with a focus on Europe, in June 2020. Upon his arrival in Portland, he had not yet produced an analytical product. Moreover, the analyst had previously been with OSCO, and he may have volunteered for deployment thinking that he would be performing tasks in Portland relating to that prior experience. Instead, the CTMC analyst was given a project whose purpose was to try to identify who was behind the violence occurring in Portland. The analyst did not feel he was well-equipped for this job and had concerns about the sources and methodology upon which he could rely, namely Field Intelligence Reports (FIRs).[364]

---

[360] Ex. B16 (Email, CETC Director to FOD RD, subject: Re: Deployment Request, July 29, 2020 3:30 AM). This email chain also shows that the OSCO Branch Chief's actual departure date may have been July 29, not the 28th, although that would still not be contemporaneous with OSCO's operation already winding down.
[361] Ex. A17.
[362] *Id.*
[363] Ex. A19.
[364] Ex. A75.

The July 28, 2020 note from the Regional Director of Portland to the Director of CETC also reveals the possibility that I&A may have been planning on sending additional OSCO collectors to Portland, before its controversial activities were revealed in the leak of the three OSIRs. One additional volunteer had apparently already been identified for rotation into Portland.[365] The only other potential corroboration for the possibility that new OSCO collectors would have been surged to Portland but for the revelation of the OSIRs are the observations and conduct of Collector #2, as told by him. According to Collector #2, sometime shortly after the OSIRs were leaked, the remaining collectors had come to their own conclusion that there were numerous reasons why they should not remain in Portland and that OSCO should not send other collectors to replace them. They decided that they should confront their Branch Chief with this recommendation, especially noting the fact that civil unrest had abated and the leak of the OSIRs may have tainted OSCO in the eyes of the Federal partners with whom the collectors were co-located.[366] Note, however, that none of the other OSCO collectors who were with Collector #2 at the end of the deployment mentioned anything about the team confronting CETC management in this manner.[367] Collector #3 thought that the team would be staying through August, but then were suddenly redeployed.[368]

Ultimately, the OSCO team was brought back home and no collectors were sent to replace them. FOD continued to provide support at a diminished level. When the investigation team interviewed the Regional Director for the Pacific Northwest in November 2020, she said that Portland continues to be staffed by an I&A employee from (b) (7)(C), (b) (6). On December 1, 2020, the Acting Director for FOD confirmed that Portland was being filled with a permanent hire as of December 7, 2020.[369]

### C. The Three Leaked OSIRs, Operational Background Reports, and Device Exploitation

Three OSIRs OSCO published during the deployment to Portland raised significant concerns. Specifically, OSIR-04001-0932-20, OSIR 04001-0937-20, and OSIR-04001-0952-20, all of which were later recalled, should not have been published in the first place, and if appropriate safeguards were in place, their publication could have been prevented. Most significantly, no collection requirement and no apparent intelligence mission supported the collection of the information that was included in any of the three serialized reports. In addition, insufficient masking of USPI drew focus from what was ostensibly the intended subject matter of the OSIRs and raised First Amendment concerns. The OSIRs documented USPER journalists publishing unclassified information that was supplied to them, which is activity protected by the First Amendment. While interviews revealed that the individuals within OSCO who identified and published the information at issue were not motivated by a desire to prevent or focus on First Amendment protected activity, the OSIRs were nevertheless problematic and should not have been published. Several overlapping institutional deficiencies led to the publication of the three

[365] Ex. B28 (Email, OSCO Collector to OSCO SDO, subject: Re Portland, July 28, 2020 10:24 PM).
[366] Ex. A52.
[367] Ex. A6, A43, A72.
[368] Ex. A43.
[369] Ex. A9.

OSIRs at issue. To provide full context of the circumstances that led to the publication of these OSIRs, a thorough description of their publication is presented here.

1. OSIR-04001-0932-20

On July 24, a collector deployed to Portland[370] noted the I&A leadership interest in leaks (which is described in greater detail below) and added terms regarding leaks into his search queries. As a result, he found the leak of an email from I&A leadership to the workforce. He was not sure how OSCO handled leaked documents. He showed the post with the leak to the OSCO Branch Chief. The Branch Chief notified the Director of CETC, and they instructed the collector to promulgate an OSIR right away. The Branch Chief instructed the collector to call the content manager and have the content manager start working on it. The Branch Chief also told the collector that there was a requirement for leaks, and the collector should use it. The collector wrote the OSIR and had a colleague conduct peer review. He had never looked for a requirement for leaks before, but he knew a colleague had worked on an OSIR regarding leaks, and the Branch Chief had said there was a requirement for leaks.[371]

The collector called the content manager and conveyed that an OSIR was forthcoming and leadership wanted the OSIR to go out right away. The collector asked the content manager to insert the requirement, because the requirement was classified and the collector did not have access to the classified system in Portland. The collector assumed the content manager would know the requirement.[372]

In response to questions during this review, the collector also stated that he was unsure of the masking procedures. He stated that the guidance regarding masking was inconsistent; he would ask questions and get different answers depending on who he asked, and sometimes he received different answers from the same person on different days.[373]

The collector received an email from I&A leadership thanking him for identifying the leak.[374]

The content manager who processed the first OSIR stated that on that day, he had worked a long day, left work at about 10:00 p.m., drove home, "crawled into bed," and was roused from sleep by the phone call from the junior collector who informed the content manager that the CETC Director said this report needed to go out right away. The content manager reviewed the report, and looked at the attachment to make sure the attachment matched the body of the report. He saw the information matched, and he noted there were some redactions. He stated that since he

[370] The collector started at OSCO shortly before the civil unrest began. The collector had received instructions to read the cookbook, a few emails about the threats to look for, a few calls with his supervisor and CETC leadership, and some on the job interaction with other collectors. This collector had some on the job training, but had not received formal training. Ex. A52.
[371] Ex. A52.
[372] *Id.*
[373] *Id.*
[374] Ex. B1 (Email Acting DUSIEO to [Collect #2], subject: Fwd: DHS I&A Email Leak, July 25, 2020)(stating in part "Nice job, [Collector #2]!").

had been instructed to get the report out the door, he published the OSIR and went back to bed.[375]

The content manager stated that he missed the reporter information in the attachment. Per his general practice, he "absolutely" checks attachments; he stated that missing the reporter's information "was a complete oversight on [his] part." There was no mention of reporters in the body of the report. The reporter's information was in the attachment. He saw that there were redactions in the attachment, but he just missed the reporter information. "If I had seen it, I would have made sure I stopped it."[376]

The content manager provided context for the publication of the OSIR. The content manager recalled that at that time he felt "sleepy," "overworked" and "pressured." At the time all these things were happening, upper management "did not want to hear any excuses;" they just wanted numbers. They wanted him to get OSIRs published. That was the priority. At that point, he was so overwhelmed he was "basically a zombie," and he was just processing as quickly as he could.[377]

The content manager stated that typically, OSCO would not report on leaks. If collectors discovered leaks while going about their work, the standard practice was to instruct them to send the leak information to the Chief of Security (CSO). However, this issue arose during a stressful time, in the middle of the night, with instructions from the CETC Director to get the OSIR out, and the content manager was also focused on the fact that the collector did not know which requirement to use. As he recalled, the collector looked at a requirement that was used for another leak and listed that requirement.[378]

The next day he was in the office, the content manager emailed a colleague to ask if there was a requirement for leaked government documents. That colleague was working remotely and had to ask someone else to check. At some point they decided there was no requirement for leaked FOUO I&A documents.[379] But by that time, the second OSIR had already been published, and the content manager who published the third OSIR was not aware of the discussion regarding the collection requirement. This all happened within a few days with much miscommunication between Friday, July 24, and the following Wednesday.[380]

The content manager did not initiate the recall process for the OSIR at that time. He took into account the fact that the direction to publish the OSIR came from such a high level, that there can be some gray areas with respect to collection requirements and the listed one was in a related area, and in his mind, there was only one OSIR impacted and it was "one and done." He did not think about the OSIR again until it was brought to his attention that the OSIR included "the reporter or the company he worked for." He took another look at the OSIR and said, "it does not

[375] Ex. A64.
[376] *Id.*
[377] *Id.*
[378] *Id.*
[379] The review team has confirmed that there was no collection requirement that would cover the unauthorized disclosure by an I&A employee of an internal FOUO I&A document to an USPER member of the media.
[380] Ex. A64.

mention the reporter." But then when he looked at the attachment again, he saw the information in the header. He stated that he realized that he had just overlooked the information.[381]
A member of the review team reviewed the classified Essential Elements of Information (EEI) and the OSIRs and determined that the listed collection requirement did not apply. The EEI was inapplicable for two reasons: the topic of the OSIR did not align with the listed EEI targets or scope. The Acting DUSIEO and CMD Director both concurred that the EEI did not support the collection.[382]

2. OSIR-04001-0937-20

The collector who found the first leak still had the same search terms running, and he also found the second leak. This time, the leaked document was an email from I&A leadership regarding use of the terms violent opportunist (VO) and violent antifa anarchists inspired (VAAI). Once again, the collector showed the Branch Chief what he had found. The collector drafted the OSIR and used the same requirement that had been used for the first OSIR. He went through the peer review process again, this time with a different colleague. Then he sent the draft OSIR to content management.[383]

On the morning of Sunday, July 26, a content manager different from the one who processed OSIR-04001-0932-20 received a request to review and publish an OSIR as soon as possible. The content manager read through the draft and pushed it through. The content manager could not recall whether she raised a question about the collection requirement; at that point, everyone was operating quickly. In addition to working every day, the content manager was concerned about the well-being of the collectors in Portland and was focused on moving quickly to address requests from Portland and not wasting time.[384]

The content manager stated that the collector, the person conducting the peer review and the desk officer are all expected to check the collection requirement. However, the second OSIR cited the same collection requirement as the first OSIR. Given that the two concerned the same topic, a leaked unclassified I&A email message, no one saw the need to recheck the collection requirement.

3. OSIR-04001-0952-20

The same collector who wrote the first two OSIRs wrote the third on July 28, 2020. This one was a little different, because an unclassified I&A product had leaked. It was also different because the leaked document was embedded in a news article. In light of these differences, the collector was not sure whether the same process would apply. He showed the leak to the Branch Chief and she instructed him to write it up.[385]

[381] *Id.*
[382] Ex. A12, A44.
[383] Ex. A52.
[384] *Id.*
[385] *Id.*

The content manager who published the third OSIR was publishing about 20-30 reports a day. That content manager stated that there was a lack of direction and guidance from leadership. It was a busy time, and they were pushing things out unless there was something blatantly wrong. Moreover, this content manager did not have access to the high side collection requirement, and was therefore unable to double-check that aspect of the OSIR.[386]

4. Conditions That Contributed to the Publication of the Three OSIRs

Several overarching pressures contributed to the environment in which the three OSIRs at issue were published.

First, I&A's focus on leaks contributed to the publication of the OSIRs at issue. Over the last couple of years, I&A had an issue with the unauthorized release of unclassified FOUO materials.[387] The leaks were the subject of conversations and a source of concern for I&A personnel.[388] Mr. Murphy was concerned about the leaks;[389] one individual described Mr. Murphy as "preoccupied" with the leaks.[390] Every time the I&A front office became aware of a leak, information regarding the leak was captured and provided to the CSO and the DHS OIG, who were the entities authorized to and responsible for investigating unauthorized disclosures.[391] Mr. Murphy specifically provided standing directions to his staff to report all leaks to the OIG.[392] These practices predated the recent in-depth training at I&A regarding the Whistleblower Protection Act.[393]

With respect to the events that occurred during the deployment to Portland (which predated the recent training on the Whistleblower Protection Act), the CETC Director and OSCO Branch Chief both directed the creation of OSIRs regarding leaks.[394]

Second, OSCO's shift to focusing on OSIRs relating to duty to warn meant that their normal operational tempo required immediate action to prevent threats.

Third, I&A leadership was particularly focused on the civil unrest in Portland, and everything relating to it was treated as being urgent. Multiple people interviewed stated that Mr. Murphy wanted everything done immediately; there was no normal battle rhythm and he expected his instructions to be carried out right away.[395]

These pressures created an environment in which everything was urgent. CETC leadership conveyed that sense of urgency. This is the context in which it was not outside the norm for a

[386] Ex. A35. The content manager who processed OSIR-04001-0952-20 had returned to CETC temporarily from his current position to help CETC process the enormous backlog that had built up.
[387] Ex. A2, A14, A17, A24, A45, A63.
[388] Ex. A6, A14, A17, A21, A24, A28, A56, A76.
[389] Ex. A46.
[390] Ex. A2.
[391] Ex. A24.
[392] *Id.*
[393] *Id.*
[394] Ex. A6, A43, A50, A52, A58.
[395] Ex. A44.

junior collector to be instructed to wake a content manager to request that he immediately publish an OSIR regarding an unclassified email that had been published and leaked. No one questioned the need for immediate publication or pushed back – this operating tempo that dictated immediate action was the overarching consideration.

This environment did not allow for normal procedures that could have prevented the publication of the OSIRs. For example, although numerous individuals stated that the standard process to address a leak would have been to alert the CSO rather than publish an OSIR, that process was not followed with respect to the three leaks identified in Portland.

In addition, Collections Management was not consulted until after the first OSIR was published. Shortly after Collections Management was consulted, a Branch Chief within Collections Management advised OSCO that he was not familiar with any OSINT requirement related to leaked documents and memoranda and expressed doubt that a general requirement along those lines would be cleared by the oversight offices. The Director of Collections Management advised I&A leadership that the collection did not fall within the bounds of the requirement.[396] Collections Management unambiguously advised OSCO leadership and I&A leadership that the collection requirement at issue did not extend to leaks of FOUO I&A materials. The collection requirement cited was inapplicable; it did not match the subject matter of the OSIRs.

On rare occasion, it could be appropriate to create or update a collection requirement if a collector identifies information that fills an intelligence gap but for which there is no requirement. If a collector conducting appropriate collection efforts comes across information that pertains to a national or departmental mission for which there is no collection requirement, that collector can hold the information in order to coordinate with the relevant mission center and collection management to determine whether it would be appropriate to modify an existing collection requirement or pursue the creation of a new collection requirement.[397] However, in that rare circumstance, the OSIR would not be published until the collection requirement was in place, following appropriate coordination and review by the oversight offices.[398] Here, there was no significant effort to pursue a new collection requirement, and those consulted expressed some doubt that a collection requirement that would cover these leaks would be approved. If the OSIR had not been published immediately, these significant issues could have been raised. As it was, when these concerns were raised, the OSIRs had already been published and leaked.

It would not be problematic for OSCO collectors to notify their leadership if, in the course of conducting appropriate collection, they identified unauthorized disclosures of unclassified DHS information. Moreover, it would not be problematic for I&A to notify the offices within DHS responsible for investigating potential insider threats (e.g., DHS OIG and the CSO) if they became aware of the unauthorized disclosure of internal DHS information. This would be equally true for I&A information and other DHS information. However, internal notification that potentially sensitive internal information was leaked is distinct from serialized reporting on a leak.

---

[396] *Id.*
[397] Ex. A40.
[398] *Id.*

The specific issues regarding the creation and dissemination of the three OSIRs at issue were (1) OSCO leadership did not appropriately train its collectors on how to create search terms or monitor the search terms employed, resulting in a situation in which a junior collector utilized search terms specifically designed to identify leaks of unclassified information; (2) the OSCO Branch Chief and the CETC Director instructed the junior collector to create an OSIR for each identified leak instead of just reporting the leak to the CSO; (3) the manufactured urgency, coupled with the late hour and limited access to classified EEIs created a situation in which the first OSIR identified an inapplicable EEI; (4) the content managers who published the later OSIRs relied upon the EEI listed in the first OSIR instead of independently reviewing the applicable EEI; and (5) the OSIRs were not immediately recalled after it was determined that there was no applicable EEI.

5. Operational Background Reports ("Baseball Cards")

On or about June 3, 2020, Mr. Murphy directed CETC to prepare operational background reports (OBRs), or "Baseball Cards"[399] as they were colloquially referred to within I&A, on protestors arrested allegedly for committing federal crimes in connection with the ongoing civil unrest in Portland. Convinced that there was a coordinated effort to commit violence, Mr. Murphy's intended purpose was to use the OBRs to confirm his suspicions that a link existed amongst the arrestees and identify a single individual or group that was "masterminding" the attacks.[400] Mr. Murphy conveyed the new directive verbally to the CETC Director with little to no guidance on execution. CTMC was tasked with producing a link analysis to determine if the arrestees were connected.[401] The OBRs essentially amounted to dossiers on USPERs which would be disseminated to I&A leadership, FOD, FPS, and the Acting Secretary, although some believe that the distribution included SLTT partners.[402] CETC leadership conveyed the tasking to CETC staff on June 4, 2020 via email stating that the Acting USIA tasked CETC with creating "a baseball card EVERY TIME there is a confirmed attack on law enforcement officers."[403]

CETC leadership sent an email describing the intended workflow for the newly mandated product. The subjects for the OBRs were provided by FOD.[404] The Watch was tasked with

[399] A baseball card is a term of art common in the intelligence community and is typically a one-page document created to provide a snapshot and brief history of any derogatory information. Ex. A3, A19.
[400] Ex. A9, A11, A12. During questioning, Mr. Murphy advised that the Acting DHS Secretary (AS1) and the Acting DHS Deputy Secretary (AS2) drove the decision to produce OBRs and initially wanted I&A to create OBRs against everyone participating in the Portland protest to which Mr. Murphy advised I&A could only look at people who were arrested to support the department, an activity they had done "thousands" of times before. According to Mr. Murphy, AS2's request was predicated on a supposition that a certain USPER was funding the violence in Portland. Ex. A46. However, during an email exchange on July 25, 2020, Mr. Murphy proclaimed that the AS1 and AS2 "has never given me any direction on what to do regarding threats." Ex. B40 (Email, Brian Murphy to ILD, subject: Immediate Change of Definitions for Portland, Saturday, July 25, 2020 8:53 PM). Furthermore, as is further discussed, some OBRs were conducted on persons arrested having nothing to do with homeland security or threats to officers.
[401] Ex. A9, A11.
[402] Ex. A18, A46, B25 (Email, CETC Director to staff, subject: RE: Immediate Review, Wednesday, June 10, 2020 10:00 AM), B35 (Email, CETC Director to staff, subject: NEW Requirement for Action, Thursday, June 4, 2020 9:50 AM).
[403] Ex. B35 (Email, CETC Director to staff, subject: NEW Requirement for Action, Thursday, June 4, 2020 9:50 AM (emphasis in the original)).
[404] Ex. A43.

completing the top section of the OBR template which encompassed derogatory information, travel history, including the individual's U.S. passport number, and immigration status.[405] They ran the USPERs through various systems such as (b) (3)(A) (ii), TECS, LexisNexis, and ATS to conduct their searches.[406] OSCO was responsible for filling in the social media section, which was accomplished using Tangles, a social media aggregation tool that compiled information from the subject's available social media profiles.[407] The two were merged together to form the complete OBR and sent to CETC leadership for review. Once cleared, the Watch disseminated the final product.[408] During the initial stages of the Portland deployment, FOD was responsible for distributing the OBR to FPS. However, CETC assumed that role midway through the deployment.[409] FPS is not a member of the intelligence community.[410]

Initial drafts of OBRs completed by OSCO personnel included friends and followers of the subjects, as well as their interests. Just the collection of names of USPERs found on social media profiles could be a violation of those individuals' privacy rights under the IO guidelines if the appropriate reasonable belief standard and mission need are not satisfied.[411] Fortunately, early drafts of OBRs removed this information and replaced it with "friends list available upon request." However, the subject's interests and some of their First Amendment speech activity (posts) were still collected.

A number of CETC staff voiced significant concerns over the legality of such an intrusive collection of mass amounts of USPER information on protestors arrested for trivial criminal infractions having little to no connection to domestic terrorism.[412] For some, the concern was so grave that they refused to work on OBRs altogether.[413] In response to staff objections, CETC leadership sternly rebuffed the staff during a July 16, 2020, branch call admonishing staff that justification for completing the intrusive background searches was not necessary, "requests from leadership are justification enough, don't need specifics … if he gives tasking it's clear/legal to do."[414] This exhortation, however, did not resolve the immense consternation surrounding this sensitive and invasive activity. Accordingly, some staff took their concerns to the analytical ombudsman and to ILD.

It is unclear when exactly ILD became aware that OBRs were being completed as a standard practice in connection with the civil unrest in Portland. It appears that the issue was brought to the analytical ombudsman on or around June 5, 2020, just one day after CETC leadership

[405] Ex. A61, B36 (Email, OSCO Branch Chief to staff, subject: OBR workflow, Wednesday, June 17, 2020 12:18 PM).
[406] Ex. A61.
[407] Ex. A50, A72, B36 (Email, OSCO Branch Chief to staff, subject: OBR workflow, Wednesday, June 17, 2020 12:18 PM).
[408] Ex. B36 (Email, OSCO Branch Chief to staff, subject: OBR workflow, Wednesday, June 17, 2020 12:18 PM).
[409] Ex. A18.
[410] Executive Order 12333, Sec. 1.7.
[411] IO guidelines are designed to protect the right to privacy under the First and Fourth Amendment.
[412] Ex. A65, A75, B25 (Email, staff to OSCO Branch Chief, subject: RE: Updates to Profile - due ASAP, Saturday, June 6, 2020 2:32 PM); B37 (Email, staff to CETC leadership, subject: Weak Justifications for Database checks on protestors, Thursday, July 23, 2020 6:45 AM).
[413] Ex. A37, A43, A45.
[414] Ex. B38 (Email, staff to [review team], subject: RE: 13 November Interview Documents as Requested, Saturday November 14, 2020 8:48 AM).

announced the directive to CETC staff, and the ombudsman then took the matter to ILD and the IO office for their awareness.[415] ILD was provided with a template for the OBRs and upon review, raised a number of concerns to address with CETC leadership. Chief among the concerns was the labeling of the OBR subject as an "anarchist extremist" without sufficient facts to support such a characterization, in addition to the collection of the account names of the subject's friends and followers and interest groups he or she followed.[416] ILD attempted to raise the matter with CETC leadership and Mr. Murphy, but was never given sufficient information on the OBRs (purpose, intent, dissemination) and therefore, could not definitively opine on the matter.[417] CETC leadership developed a SOP delineating the structure of OBRs and authority to produce them without consulting with ILD or intelligence oversight.[418] Nevertheless, a number of witnesses asserted that CETC leadership made repeated statements to the staff that the OBRs were "blessed by legal" in an effort to assuage their growing concerns over the activity and possibly deter staff members from directly reaching out to ILD or any of the other G4 offices.[419]

Interestingly, on July 11, 2020, a FOD employee contacted an attorney in ILD for legal guidance on the appropriateness of disseminating a prepared OBR to an Assistant United States Attorney (AUSA) in Portland. During that exchange, the employee and ILD were able to reach a conclusion that sharing the OBR with the AUSA could result in a need to appear at trial as a witness. Noteworthy, ILD explained that it previously counseled CETC on the discovery and exposure risks of sharing OBRs outside of DHS internal channels and conveyed that their understanding was that these products would not be shared beyond "I&A, or, at most, used only DHS-internal."[420] Despite this guidance, on at least one confirmed occasion, it appears CETC staff shared an OBR created on a USPER with an AUSA sometime around July 29, 2020.[421]

OBRs are certainly not new to I&A. The moniker, baseball cards, is a product that appears to have originated in HITEC, but were mostly done on non-USPERs or only done on USPERs that had a demonstrated terrorism nexus.[422] When the demand for OBRs grew too cumbersome, the task transferred to CETC, but the terrorism nexus piece still remained the predominate basis for compiling the report on an individual. This transfer occurred long before the standardized institution of them in the Portland civil unrest surge.[423] Initial requests for OBRs at the start of the surge to support DHS in quelling the civil unrest involved subjects who allegedly committed vehicular assault – vehicle ramming – on law enforcement officers.[424]

Although I&A was ostensibly supporting a departmental mission when it created the OBRs for Portland (including the FPS mission associated with protecting federal property), this authority is not unbridled. I&A's authority to collect and disseminate the information gathered on USPERs

[415] Ex. A25, A65, B25 (Email to staff, subject: RE: Concerns from CETC, Friday June 5, 2020 5:20 PM).
[416] Ex. A25, A33.
[417] *Id.*
[418] Ex. A58, A57.
[419] Ex. A45, A50, A58.
[420] Ex. B39 (Email, FOD Regional Director to ILD, subject: OSINT Team, Saturday, July 11, 2020 10:22 PM).
[421] Ex. B39 (Email (FOD Regional Director to ILD, subject: OSINT Team, Saturday July 11, 2020 11:10 PM)(same email thread, different email than the one cited immediately above).
[422] Ex. A49.
[423] Ex. A49, A75.
[424] Ex. A51, B41 (Email, CETC Director to staff, subject: USIA Request, Wednesday, June 3, 2020 9:28 AM.)

as packaged in the OBRs is governed by the reasonable belief standard. As explained in Section V above, the IO Guidelines compel I&A personnel to have a reasonable belief that the collection activity furthers one or more national or departmental missions in order to intentionally collect USPI.[425] And as further explained in Section V, ICD 107 requires the HICE to "[c]onduct intelligence activities in a manner that protects civil liberties and privacy and provides greater public transparency." This means that where First Amendment activities are implicated, I&A should tread carefully before including USPI or other potential First Amendment-protected content. The facts surrounding the collection of the USPI in the OBRs may have failed to meet the applicable standards in some instances, but this is a determination requiring further investigation by the IO Office.

One concern with the OBRs was Mr. Murphy's reason for wanting them created in the first place. As Mr. Murphy described it, the same individuals were showing up every night to protest and had a level of organization, and I&A needed the collection piece to definitively demonstrate that the violence was not random and that the individuals were connected.[426] However, hunches or intuitions are not sufficient bases for collection,[427] and without more, creating intelligence products on USPERs in an attempt to make a connection – before there was a reasonable belief that the products furthered a national or departmental mission – would have been inappropriate.

An analyst from FOD was tasked with developing a "link chart" to meet Mr. Murphy's directive. It became immediately apparent to this analyst that the OBRs "were thrown together. Didn't even know why some of the people were arrested. So I created one slide that had the dates and names of the persons arrested, no other connections."[428] The information was turned over to CTMC to continue with the link analysis, "but there was nothing for CTMC to add with respect to the people identified as connected to the civil unrest; those individuals were not international terrorist subjects, they did not hit on the systems, and they were not flagged as domestic terrorists. CTMC never published anything externally because they did not find any links. CTMC's strength is strategic analysis, not identity-focused analysis."[429] Likewise, HITEC was tasked with conducting a connection analysis to "determine if [the subjects] were part of some larger network that was directing or financing them," but they did not find any evidence that assertion was true.

Another concern with the OBRs is the amount of information provided in the OBRs about arrestees to connect their arrests to a national or departmental mission. A review of 43 OBRs[430] provided during the course of our investigation reveal that on at least seven occasions, arrestee

[425] DHS I&A Instruction IA-1000, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (January 19, 2017).
[426] Ex. A46.
[427] DHS I&A Instruction IA-1000, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (January 19, 2017).
[428] Ex. A11.
[429] Ex. A13.
[430] The total number of OBRs created could not be assessed. Witnesses were unsure of the total number of OBRs created. Some stated that only 20 were produced, others stated they'd only seen 20-25, and still others claimed there were about 50-100 created. Our team was provided with a total of 43 though it is apparent that there are more OBRs than what was provided. Not all the OBRs could be recovered, as they were deleted from the share drive used to create and edit them. B13, Interview Documents Follow Up.

information is not divulged.[431] In order to satisfy the reasonable belief standard, it is insufficient that the USPER was simply arrested for *a* crime. The details of the charges of the arrest would have needed to be made known to the collector so that they could conduct a proper analysis to establish reasonable belief that conducting a records search on a named USPER would support national or departmental missions. At least one collector raised this exact concern when they were provided a list of USPERs to run background searches on without accompanying background/arrest information. The response this collector received from a fellow collector was that only the names and dates of birth for the individuals was provided, at which point CETC leadership interjected and stated that "these individuals have been arrested in connection with the civil unrest – run them."[432] However, a review of the OBR created for at least one of the individuals identified in the request show that the USPER was a "subject of interest to local Portland authorities;" no other details or arrest information was provided and no derogatory information was found.[433] It is possible this information was available to the collector but omitted from the OBR. However, when asked, several witnesses could not confirm any arrestee information for this particular subject.[434] One witness commented that sometimes the list of names provided had arrest charges and sometimes it did not, they never saw an arrest affidavit or paperwork, they just worked off of the assumption that everyone on the list was arrested.[435] One could counter that I&A was authorized to collect information on USPERs in these instances because they reasonably believed it furthered the departmental mission of FPS, a DHS component. There is no contention that I&A can't support FPS in its mission, however, as a member of the intelligence community and therefore subject to Title 50 of the United States Code and Executive Order 12333, I&A's authority to support departmental missions is not unbridled. Any intelligence activity, especially activities that infringe upon the privacy rights of USPERs, must be conducted with regard to the civil liberties and privacy rights guaranteed by laws and policies protecting individual privacy.

In some cases, the arrests noted in the OBRs appear to have been related to a departmental mission. For example, there were a number of OBRs created on subjects who were arrested for assaulting federal officers – shining lasers in officers' eyes, throwing Molotov cocktails or other objects towards federal property or federal law enforcement officers – and at least one report that was prepared on an arrestee who was a suspected member of ANTIFA. Although it is unclear whether these OBRs provided any significant benefit, they are less concerning than others.

Certain OBRs on individuals arrested for other crimes are also concerning. For example, of the 43 OBRs provided to the review team, 13 were identified as arrests for nonviolent crimes.[436] Although nonviolent crimes may be related to a national or departmental mission, that connection is unclear from the OBRs. A number of the subjects arrested for nonviolent crimes were charged with trespassing or failure to comply. There was insufficient information available as to whether the arrests were made by FPS or state or local law enforcement. Additionally, it is

[431] Ex. B68-73, B52 (Operational Background Reports Re USPERs 1-6, and 10).
[432] Ex. B74 (Email to staff, subject: Background Check for Two OBRs, Thursday, July 16, 2020 4:48 AM). At least one witness claimed that an OBR would be requested for individuals that were not arrested, just those who made a threat, such as if the USPER simply made a threat to a federal building or DHS personnel. See Ex. A36.
[433] Ex. B75 (Operational Background Reports Re USPER 7).
[434] Ex. A36.
[435] Ex. A55.
[436] Ex. B51, B53, B54, B56-B65 (Operational Background Reports Re USPERs 9, 11-15, 17-23).

unclear whether there was any relationship to federal property or if the arrests for failure to comply had any connection to violent protest activity. The review team considered this activity in retrospect, but there are too many variables that needed to be resolved at the start of the collection activity before an intrusive background search on USPERs is conducted. For these reasons, further investigation by the IO Office into OBRs is needed.

In one case, CETC prepared an OBR on an USPER whose social media profile clearly identified the individual as a journalist. This individual was arrested for flying a drone in a national defense airspace. The arrestee's purpose for flying this drone was not identified in the OBR – it may have been for the purpose of capturing photographs of the ongoing activities or for some other reason – and as such it is unclear whether this OBR was a valid exercise of I&A's legal authority.[437] In another instance, an I&A employee requested a report on another journalist – the same journalist at issue in one of the leaked OSIRs – and included instructions to add "a list of any [of his] associates or groups."[438] The journalist in that case had not been arrested for anything, but had posted unclassified DHS internal correspondence to his social media page. In addition to poor optics, completing an OBR on this journalist without a clear connection to a national or departmental mission arguably would have failed to satisfy the reasonable belief standard. Fortunately, a collector recognized that the subject was a journalist, alerted the requestor to this fact, and declined to proceed with that particular search.[439] But the facts of this particular incident suggest that at least some I&A personnel did not understand the relevant legal standard before running checks on USPERs.

Even if the *collection* of USPI was proper in all the aforementioned circumstances, I&A also needed to establish a reasonable belief to retain the information permanently. If I&A personnel cannot establish a reasonable belief for permanent retention of USPI, it must be purged within six months of collection.[440] Accordingly, in those instances where a link to a national or departmental mission cannot be identified, the OBRs need to be deleted. Ideally, they should be deleted upon completion of evaluating whether the USPI qualifies for permanent retention. Given that most of the OBRs reviewed were collected and prepared in June and July, the six-month temporary retention period expires either December 2020 or January 2021.

In order to disseminate the OBRs, the USPI would have had to be permanently retainable, must satisfy a mission need, and the intelligence personnel needed to have a reasonable belief that "dissemination would assist the recipient of the USPI in fulfilling one or more of the recipient's lawful intelligence, counterterrorism, law enforcement, or other homeland security-related functions."[441] For reasons previously discussed, it is questionable whether at least some of the OBRs satisfied the permanent retention requirement and mission need. There are no constraints

[437] Ex. B63 (Operational Background Report Re [USPER] 23).
[438] Ex. B66 (Email to staff, subject: RE: (U//FOUO) OSIR-04001-0937-20 - Social media user posts a leaked Department of Homeland Security internal memo that discusses changing terminology used in reports, Sunday July 26, 2020 1:50 PM).
[439] Ex. A51, B66 (Email to staff, subject: RE: (U//FOUO) OSIR-04001-0937-20 - Social media user posts a leaked Department of Homeland Security internal memo that discusses changing terminology used in reports, Sunday July 26, 2020 1:50 PM).
[440] DHS I&A Instruction IA-1000, Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (January 19, 2017).
[441] *Id.* at § 2.3.

with disseminating USPI internally within I&A as long as the recipient has a need to know, and that is not at issue here. Therefore, we find no fault in sharing the information within I&A with the Acting Under Secretary and FOD. However, FPS, AS1, AS2, and AUSAs are not members of the intelligence community.[442] Therefore, in instances where permanent retention and mission need could not be satisfied, dissemination to these entities would not have been proper.

I&A's Intelligence Oversight Office is currently conducting an investigation into the activities surrounding the OBRs to determine, *inter alia,* whether the activities surrounding the OBRs are reportable as a Questionable Intelligence Activity.[443]

6. Exploitation of Protestor Devices

During the I&A deployment to Portland, FPS asked I&A HITEC to exploit devices seized from protesters by FPS, but I&A did not do so because FPS never met the necessary legal conditions for I&A exploitation.[444] On July 14, SOPDPDUSIA Jen instructed HITEC to send a team to go to Portland to exploit devices,[445] and to leave the next day.[446] The Regional Director on the ground in Portland at the time and the HITEC Director both agreed that deployment was not advisable or warranted.[447] After HITEC leadership discussion with the Acting DUSIEO and ILD,[448] the deployment was canceled. The SOPDPDUSIA did direct the HITEC Director to coordinate with the FPS incident commander to ascertain whether there were any devices, to identify the status of the devices, and determine what legal authority FPS possessed to hold the devices.[449] In order for HITEC to engage in device exploitation, "the first step is that FPS has to have the authority to seize the devices, and then FPS has to decide whether FPS has the authority to share the devices with I&A, and then I&A has to determine whether I&A has the authority to collect the information from the devices."[450] These requirements generally translate into the necessity for a having a warrant and sending a written request to I&A for assistance. FPS provided neither.[451] As such, I&A never possessed the devices or any information from the devices and exploited no information from the devices notwithstanding regular inquiries from SOPDPDUSIA Jen and the Acting USIA Murphy as to why HITEC had not exploited those devices.[452]

In addition to devices in FPS's possession, the Portland Police Bureau (PPB) also apparently possessed cell phones obtained from individuals that PPB had arrested.[453] According to FOD's Deputy Director (East), a FOD IO was asked to send an email to the Chief of PPB that I&A had

[442] E.O. 12333, Section 1.7; Ex. A2, A25.
[443] Ex. A2, A25.
[444] Ex. A49
[445] *Id*.
[446] Ex. A69, Sending HITEC to Portland didn't make logistical sense since all of their tools are only in Washington and the only action that their team would be taking is sending the devices or its data back to DC. Ex. A49.
[447] *Id*.
[448] Ex. A49.
[449] *Id*.
[450] *Id.*
[451] *Id.*
[452] *Id.*
[453] Ex. A56, A68,

the capability to exploit cell phones.[454] This offer of assistance was never taken up by PPB.[455] The matter of cell phone exploitation as it related to PPB was mooted after the Portland City Council passed its resolution instructing PPB to not cooperate with DHS.[456]

### D. I&A Work Environment

#### 1. Work climate.

The work climate at I&A was not only oppressive for I&A employees, but it created the ideal conditions for questionable intelligence activities to occur.

Work climate is generally set or heavily influenced by the leader of the section, office, component, or department. Based on our review of documentation, communications, and scores of interviews, it is clear that Mr. Murphy created a toxic work environment at I&A. Some of the morale issues at I&A can be ascribed to the new strategic direction and reorganization into which first Mr. Glawe and then Mr. Murphy pushed I&A. However, leaders can accomplish organizational change without berating, castigating, and demeaning employees on a consistent basis, as did Mr. Murphy. In fact, some persons noted that one on one, Mr. Murphy could be completely reasonable by listening to whatever proposal was made. Others noted he could be quite personable.[457] Unfortunately, Mr. Murphy also regularly interacted with I&A personnel by criticizing and haranguing subordinates and junior analysts in public (euphemistically referred to as getting "Murphed"), refusing to listen to counter viewpoints, abruptly making decisions, and ignoring data that did not comport with his perceived analysis.[458]

The excerpts below were selected from the interviews of the most senior I&A leaders (one from outside I&A), all with over 20 years' experience, most with more. The only senior leader who did not express a negative view of Mr. Murphy's behavior as a leader was the then-SOPDPDUSIA Jen, on detail from another agency.

> **Exhibit A24.** A leader should be able to adapt. Mr. Murphy had challenges adapting to the leadership styles of his staff. Mr. Murphy had a specific leadership style. Some people called him a bully. That was difficult. I think it would be challenging for the organization to have Brian back.

---

[454] *Id*.
[455] *Id.*
[456] Ex. A69; B18 (Email, OCSO Director to CETC Director, subject: Re Portland City Council Resolution, July 22, 2020 9:18 PM).
[457] Ex. A19, A79. Mr. Murphy provided through his attorney the names of 18 persons as character witnesses who ostensibly could provide favorable feedback regarding the command climate created by Mr. Murphy. Ex. B43, (Email, Mark Zaid to [review team], subject: Re: Brian Murphy Interview Follow-Up, Tuesday, Dec. 15, 2020 6:03 PM). Interestingly, none of those persons selected by Mr. Murphy overlap with the names of the 79 persons interviewed for this review – persons that were selected because of their relevance to this review. At any rate, none of the persons referenced by Mr. Murphy were interviewed by this review because those witnesses already interviewed form the bulk of I&A's current leadership, and the toxic work environment and fear of reprisal that Mr. Murphy created is not offset by his character witnesses.
[458] *See, e.g.,* in addition to the statements in text, Ex. A13, A22, A38. *See also* B49 (Memorandum for Record, subject: Brian Murphy, dated December 8, 2020).

> **Exhibit A33.** Regarding command climate, employees were afraid to not deliver what was asked and afraid to push back if what was asked was inappropriate. People were routinely publicly criticized for raising questions. Mr. Murphy had a leadership style of intimidation that he tried to extend over people not even in his chain of command. He had no patience, no planning, no thought.
>
> **Exhibit A54.** But I will tell you, with no overstatement, he was by far the most toxic leader that I have ever seen. He was a disgrace to the SES. Level minus one leader of do it this way or find another job. That is him to a T. If you don't do it his way, you can find another job or no longer be invited to the meetings. Toxic person. Not a jerk to me personally at least not to my face. I had no personal run-ins with him. Smart guy. He was asking questions. We had some issues with objectivity with the Secretary's office and he defended the agency's position, which was good. But whatever good there was completely overshadowed by his lack of ability to listen or do anything corporately.
>
> **Exhibit A56**. His way or no way. Mr. Murphy is not open to feedback or dialogue, such as when he is told that a short-term solution could have long term or unintended consequences.
>
> **Exhibit A63.** Candidly, he is brilliant and articulate, but he has no regard for employees. He refuses to listen. He needs to go someplace else. No one wants to work with him; he is a jerk.
>
> **Exhibit A67**. Mr. Murphy was difficult – probably the most difficult boss [I have] ever worked for. He could not be pleased. Although Mr. Murphy could be friendly at times, you just knew when you were going to get a "headshot" – which has happened to me many times. This was described as "getting Murphed" in front of plenty of witnesses. The others present would generally stay silent. Mr. Murphy had a specific task he wanted and you had to do it. Afterward, Mr. Murphy would act as if nothing had happened, even though the incident had been brutal. This type of behavior from Mr. Murphy had a 100% chilling effect on feedback.
>
> **Exhibit A71.** Brian had an outstanding analytic mind and great intellect, but as a leader he was piss poor with zero people skills. His leadership style was to execute in public and crush dissent. As such, folks were not willing to raise their head above their foxhole. From my perspective, the fear factor ran rampant in I&A.

Accounts of Mr. Murphy as a toxic, intimidating and retaliatory leader are extremely concerning. They are inappropriate for any member of the senior executive service, and in particular one who supervises an organization of over 600 employees. At a minimum, these behaviors adversely affected the employees at I&A that we interviewed. Moreover, some of the reported behaviors could form the basis for harassment or hostile work environment claims against the Department.

In addition to the adverse effect on employee morale and productivity, Mr. Murphy's leadership approach created an atmosphere where subordinates felt that they had to circumvent what he told them to do. For example, Mr. Murphy would demand requirements divorced from I&A's mission.[459] Unable to confront Mr. Murphy with the error of his requests, employees would

[459] Ex. A44.

work around the edges to seemingly provide him the product or requirement requested. Mr. Murphy's refusal to entertain opposing opinions or staff input led to abrupt decisions that employees considered counter to existing policy or law (see VAAI discussion below). This attitude required employees to independently evaluate the directions given and decide whether to follow that direction. Doing so creates an obvious adverse effect on confidence in leadership and a drag on efficiency.[460]

The work climate created by Mr. Murphy also led to serious missteps by I&A in performing its intelligence function. In the three months that Mr. Murphy was the Acting USIA, three questionable intelligence activities occurred: collection, retention, and dissemination of OSIRs with no valid collection requirement or mission requirement; collection, retention and dissemination of USPI improperly collected for OBRs; and the potential violation of the Intelligence Oversight Guidelines regarding the promulgation of the "Violent Antifa Anarchists Inspired" term. Mr. Murphy directly or indirectly set the conditions for each of those events through his refusal to entertain counter opinions and a failure to consider staff input once he decided on a course of action, however precipitous.[461]

Regarding whether Mr. Murphy was aware of the effect that his actions had on the workforce, Mr. Murphy states that while serving as the PDUSIA, Mr. Glawe never counseled him for micromanagement and that he only heard positively about his leadership style from Mr. Glawe.[462] However, the person then serving as DUSIEO stated that Mr. Glawe understood Mr. Murphy's management weaknesses and had many discussions with him. Mr. Glawe tried to improve Mr. Murphy's management leadership style.[463] Further, another senior leader, in a position to observe, stated that Mr. Glawe had conversations with Mr. Murphy about "getting too far into the weeds." He stated that Mr. Glawe tried to bring Mr. Murphy into the "executive level of doing business" and to be an executive rather than a first line supervisor.[464] Finally, yet a third senior leader who spent extensive time with him, states that Mr. Murphy is "very aware that is who he is as a person" and "very self-aware," and that he recognizes the negative impact his style has on a workforce but makes no effort to change it.[465]

When asked about the work climate he created, Mr. Murphy did not acknowledge any issues with his leadership at I&A. He claimed to be unaware of many of the complaints against him. Nor did Mr. Murphy concede that anything about him or his leadership contributed to the issues identified in this report. Indeed, Mr. Murphy consistently placed blame on prior mismanagement of I&A, DHS leadership, his subordinates, and other offices at DHS. None of the witnesses or Mr. Murphy himself suggested that he would do anything differently if he were to return to I&A.

---

[460] Ex. A11, A13, A17, A67.

[461] When asked in an interview during this review what he would have done differently regarding Portland, Mr. Murphy did not say that he wished he had better awareness of OSCO's training, or personnel issues; he did not state that he wished for a climate that would have promoted the deliberate review of the OSIRs; he did not express any remorse for the adverse effect that the OSIR incident had on the organization; Mr. Murphy stated, "I wish I had filed my whistleblower complaint sooner." Ex. A46.

[462] Ex. A46.

[463] Ex. A28.

[464] Ex. A24.

[465] Ex. A12.

2. Employee Concerns About Retaliation.

At the beginning of the investigation, while the members of the investigatory team were still interviewing junior members of I&A, those persons interviewed immediately expressed concern regarding who in the leadership chain of command would read their statements. Interviewees explicitly or implicitly expressed concerns regarding retaliation. As such, the investigatory team changed its introduction to state at the beginning of each interview that the persons who would have access to the statements would be the current SOPDUSIA and his senior special assistant, the Acting General Counsel and a Deputy General Counsel, and the Acting Secretary and Acting Deputy Secretary. The investigatory team specifically noted that no witness statements would be affirmatively provided to Mr. Murphy unless required by law or court order. The foregoing statement alleviated the majority of the concerns expressed by those interviewed.

However, such was the toxic work climate created by Mr. Murphy, that of the 19 or so senior leaders interviewed, five expressed specific concerns of retaliation, three stated that he could not affect them because they were retiring, two noted that they were outside his supervisory chain, and two requested to amend their statement. A number of junior staff officers also expressed concern notwithstanding receipt of the statement above. In several cases, employees became overtly circumspect when they learned that under certain circumstances Mr. Murphy might have access to the witness statements. Fear of retaliation, unsurprisingly, weighed most on younger leaders and staff officers closer to the beginning of their careers than the end.[466]

3. Politicization of Intelligence Products.

This investigation revealed no evidence of politicization (roughly "write this analysis this way to support this political assertion")[467] by anyone in the I&A chain of command or DHS Secretary's office. However, Mr. Murphy did make other attempts to controvert the collection-analysis process. Particularly illuminative was the promulgation of the term "Violent Antifa Anarchists Inspired" (VAAI).

As discussed by several intelligence analysts, to understand the genesis for VAAI, one must take the events of the summer into context. In many conversations, Mr. Murphy stated that the violent protesters in Portland were connected to or motivated by ANTIFA. This may have made sense to Mr. Murphy based on his own beliefs, but I&A did not have collections (evidence) to show it and absent reporting or some other evidence on motivation, I&A analysts could not ascribe motivation to the violent actors as Mr. Murphy expected. Mr. Murphy would tell the analysts to cite to existing OSIRs as evidence of the motivation, but the OSIRs did not draw a connection to ANTIFA. For weeks, the analysts had been telling Mr. Murphy that because ANTIFA was not in the collection, it could not be put into the analysis. Notwithstanding this feedback from the I&A analysts, on July 25, 2020, Mr. Murphy sent an email to his senior leadership instructing them that henceforth, the violent opportunists in Portland were to be reported as VAAI, unless the intel "show[ed] . . . something different."[468] The analysts stated

[466] *See, e.g.*, A7; A11; A12; A24; A27; A44; A51; A56; A77; A78.
[467] *See, e.g.,* ICD 203, *Analytic Standards*, § D.4.b.
[468] Ex. B6

that "if you lived through the process, you could see where this VAAI definition was coming from a mile away. He got tired of the analysts telling him they did not have the reporting and he was convinced it was ANTIFA so he was going to fix the problem by changing what the collectors were reporting."[469]

Senior I&A leaders immediately responded negatively after Mr. Murphy summarily promulgated the term on 25 July. Several issues existed. In his email promulgating the term, Mr. Murphy asserted that

> "The individuals are violently attacking the Federal facilities based on those ideologies. We can't say any longer that this violent situation is opportunistic. Additionally, we have overwhelmingly intelligence regarding the ideologies driving individuals towards violence and why the violence has continued. A core set of Threat actors are organized, show up night after night, share common TTPs and drawing on like-minded individuals to their cause…."[470]

In fact, per the analysts' statements noted above, overwhelming intelligence regarding the motivations or affiliations of the violent protesters did not exist. Indeed, the review team could not identify any intelligence that existed to support Mr. Murphy's assertion.[471]

Further, in his statement, Mr. Murphy asserts that the VAAI term was promulgated in the same manner as the Violent Opportunist (VO) term.[472] This statement is also incorrect. The VO term was staffed expeditiously through I&A, but staffed nonetheless through all staff sections and with the FBI, before concurrence on its use occurred. VAAI was promulgated from announcement to staff on Friday, July 24, 2020 to I&A writ large on Saturday, July 25, 2020, with no formal legal analysis or staff concurrence (staff had met the day before and rejected creation of the term).[473]

The lack of legal analysis was particularly troubling to the I&A Associate General Counsel (AGC) because the definition and directed use of VAAI contradicted the IO Guidelines. The IO Guidelines state

> I&A personnel are authorized to engage in intelligence activities where they have a *reasonable belief* that the activity supports one or more of the national or departmental missions listed below.

---

[469] Ex. A14; A78; A79.
[470] Ex. B6.
[471] See discussion in Section VI.C.5 above regarding OBRs and the failure to find any link between arrested persons.
[472] Ex. A46.
[473] Ex. A9, A13, A24, A28. Mr. Murphy asserts in his statement that "he sent [the definition] to everyone else that Saturday morning. Mr. Murphy said that they talked about it and asked them to a person if they agreed with it and they did." Ex. A46. No I&A leader interviewed states that Mr. Murphy spoke to them the morning he released the definition, and all interviewed on the topic were surprised at its release. Perhaps Mr. Murphy misconstrues the requirement in his email for acknowledgement of receipt as agreement. Furthermore, given Mr. Murphy's known proclivities for reacting adversely to dissent, he should not have construed silence as assent. "The atmosphere at I&A was not one where personnel could speak up." Ex. A71.

> **Reasonable Belief**: A belief based on facts and circumstances such that a reasonable person would hold that belief. A reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge as applied to particular facts and circumstances, and a trained and experienced intelligence professional can hold a reasonable belief that is sufficient to satisfy these criteria when someone lacking such training or experience would not hold such a belief.[474]

As the Associate General Counsel for I&A stated to Mr. Murphy, (b) (5) [redacted] After strong non-concurrences from both the AGC and the Acting DUSIEO, neither of whom had been previously consulted on the decision, Mr. Murphy changed the VAAI definition from "Threat actors who are motivated by Anarchist or ANTIFA…." to "Threat actors who are *probably* motivated by Anarchist or ANTIFA…."[475] He also changed the application of the VAAI definition from a presumption to an option if the situation warranted.[476] Notwithstanding Mr. Murphy's change of position, emails were still being sent to collectors 24 hours later telling them that they must use the VAAI term.[477]

The I&A AGC thought that the VAAI issue was serious enough to require discussion with the DHS General Counsel that a questionable intelligence activity had occurred, requiring notice to the ODNI (this discussion never occurred because it was overcome by the leak of the OSIRs discussed above). Further, regardless of the definition change, "the analysts were concerned with the VAAI definition because it potentially created attribution where there was none, which would then affect the analysis. You can't pencil whip attribution."[478]

A second example of the manner in which Mr. Murphy turned analysis upside down was his dictate regarding the "Four Phases of Protest." Apparently, Mr. Murphy came to the conclusion sometime after George Floyd's death and the subsequent protests that four phases of protest exist, and he wanted to say, at least temporally, whether a protest was in a particular phase, and the indicators of that phase. As with the VAAI term, Mr. Murphy devised this idea about phases of protest on his own. From the analysts' perspective, the problem was that they were typically asked to investigate a question, not given a conclusion and told to write a paper to support it. In this case, Mr. Murphy gave the analysts the four phases and told them to find support for his proposition. Aggravating the task, they were given 48 hours over a weekend so the paper could be sent to state and local partners.[479] By requiring an artificial timeline for a product no one outside I&A had asked for, the analysts could only conduct superficial analysis, finding that the protests were all cyclical – that they could go either way, and the progression envisioned by Mr.

---

[474] DHS I&A IO Guidelines, Section 1.1 and Appendix at AA.
[475] Ex. B4.
[476] *Id.*
[477] Ex. B5; *see also* Ex. A75 regarding the requirement to use the term.
[478] Ex. A75; *see also* Ex. A9, A11.
[479] Ex. A75, A76, A78, A79.

Murphy did not occur in any predicable manner. A protest could be in Phase III and drop back to Phase II. At any rate, the paper was sent to state and local officials, where it was greeted like "a tree that fell in the forest that no one heard."[480]

4. Marginalized Oversight.

When Mr. Glawe started at I&A, his relationship with ILD was already strained due to disagreements between himself and the ILD AGC dating back to Mr. Glawe's days at CBP. Mr. Murphy became a part of these disagreements when he joined I&A. As such, the relationship between legal counsel and the I&A front office was not good and it created a "significant gap in the organization" because counsel was not at meetings where they should otherwise have been included.[481] Additionally, Mr. Murphy thought that ILD over-participated in non-legal matters, i.e., intelligence analysis. Mr. Murphy reacted by trying to cut positions from ILD (he states that he tried to cut one position; the Acting DUSIER states that he was directed to conduct review of the I&A ILD funded positions and "cut lawyers" as there were "too many").[482] Mr. Murphy would also question and castigate his staff for consulting ILD and other members of the G4.[483]

As discussed above, I&A leadership's, and in particular, Mr. Murphy's, marginalization of ILD and the other members of the G4 not only created an environment where I&A employees did not feel free to raise questions or concerns to the appropriate officials, but it created an environment where questionable intelligence activities were inevitable.

5. Employee Resilience.

Two issues existed regarding employee resilience. First is the perceived indifference that the employees who deployed to Portland felt they received when they returned to their duty stations.[484] The team members felt that they were not thanked or appreciated for their efforts even though law enforcement in Portland were especially thankful and on return, leadership insisted that they had done nothing wrong. "After we returned, there was no mention that we were back or the work they did. There was no talk about Portland at all. Everyone just kind of acted like nothing happened."[485] This created cognitive dissonance and confusion among employees; if they did nothing wrong and they did good work in Portland, then why would no one other than investigatory bodies talk about what happened in Portland. At a minimum, leadership should have discussed the deployment with those who had deployed, a process that could have occurred without impugning or adversely affecting any of the on-going investigations.

[480] Ex. A78.
[481] Ex. A24.
[482] Ex. A46; A54. Ironically, at the time of this statement, of the nine total ILD positions authorized and funded (eight by I&A and one by OGC), only six of those positions were actually filled. ILD is the second smallest legal division within OGC, supporting an I&A workforce of approximately 600 individuals.
[483] Ex. A13; A28; A44.
[484] Ex. A6; A52; A75.
[485] Ex. 52.

The second issue regarding employee resilience occurred when I&A leaders asked Mr. Murphy to hold a diversity and inclusion event. Some employees wanted to discuss issues raised by the death of George Floyd, and other workforce issues. Mr. Murphy forbid any diversity or inclusion conversations on work time. He did not understand why leaders would want to hold a meeting, and did not see a value in doing so. Mr. Murphy would not take a meeting with minority employees in regards to on-going protests on racial justice. Instead, he made SOPDPDUSIA Jen take the meeting. After Mr. Murphy was detailed, Gen. Taylor, from the Diversity and Inclusion Council, came to speak.[486]

## VII. RECOMMENDATIONS

Based on the foregoing findings, the following recommendations are made. Of note, I&A has already instituted a number of changes, especially regarding training and employee outreach. Those efforts are documented and discussed in a separate staff effort.

### A. Training

1. Reexamine Training Across I&A.

Knowledge of basic intelligence community and government underpinnings appeared inconsistent in the staff sections with whom we interviewed, perhaps due in part to the COVID pandemic, but also due to poor training models in some instances and to the decentralized training and accountability model pushed and endorsed by Mr. Glawe and Mr. Murphy, respectively, in others. New employees and supervisors are expected to be immediately able to execute their duties far before they have mastered the core competencies of their jobs. Lack of training and understanding of rules, roles, standards, and processes were major contributing factors in the improper reporting and dissemination of OSIRs. To remedy this, we recommend a reexamination of the training model and expectations for new employees and rising supervisors.

2. Certified Release Authority (CRA) training.

OSCO does not have enough CRA qualified persons. Currently, the two persons qualified as CRAs are also responsible for OSIR review, management and administrative functions for their sections (e.g., WebTA, etc.). They are the single point of failure for publication, and if and when OSIR production ever returns to a "normal," two persons using the system and process as it currently exists cannot adequately and timely perform the duties required. Training more than the number of persons required also ensures that sufficient back-up exists. Increasing the number of CRAs within OSCO (along with some other investments addressed below) would allow OSCO to publish OSIRs through all its shifts all days of the week.

3. Collector training.

OSCO is already addressing this issue with an intense live two-week training program, dubbed "Bootcamp," mandatory for all collectors, except contractors, to attend. It is taught by an OSCO

[486] Ex. A45, A54. Mr. Murphy states that he was in favor of inclusion events. Ex. A46.

employee (one of the CRAs) with segments presented by the IO office and ILD on intelligence oversight and legal principles and concepts. It focuses on tradecraft, collection techniques, and First Amendment protections. The challenge for OSCO will be to continue to provide refresher and updated training. In the course of the investigation, major gaps regarding collection affecting First Amendment issues and the Intelligence Oversight guidelines were noted with all collectors. OSCO may wish to consider revisiting those issues when "Bootcamp" ends so as to provide immediate reinforcement. Finally, although asynchronous PALMS training may more efficiently convey the same information across the three OSCO and Watch shifts, live training provides connections and humanizes the G-4 into persons with whom employees can actually contact if a problem exists.

4. Engage with the Open Source Intelligence (OSINT) field.

OSCO has not availed itself of resources beyond its organization regarding OSINT. OSINT exists as a discipline across the IC, and other elements of the IC and the private sector have numerous training opportunities. By better integrating into the larger OSINT field, OSCO would be able to set training to industry standards, learn and test their tradecraft against peers, and learn from more developed open source programs in the IC. CETC should reach out to its IC partners and avail itself of these training opportunities. CETC may also benefit from participating in an exchange program with another IC element's open source division.

5. Supervisory training for new supervisors prior to their taking their position.

New supervisors are expected to be able to lead, deal with administrative tasks, supervise, and engage in operational duties immediately upon promotion. Additionally, supervisory roles in I&A tend to be more tied to GS levels than mission need or an individual's leadership acumen. Promoting people with few leadership experiences and skills is by no means unique to I&A; however, accepting the deficiency should never become customary. New supervisors are hamstrung trying to both learn their new jobs and ascertain the resources available to learn managerial and leadership skills. Other members of the IC and DHS have mandatory supervisory training for all new supervisors. Providing this training fills in gaps, teaches key skills, instills confidence and creates a more efficient organization.

**B. Promulgate Standard Operating Procedures (SOPs)**

CETC has very few written processes, SOPs, standing orders, or directions generally. A lack of written guidance can lead to confusion, promote the loss of institutional knowledge when turnover occurs, create different training regimes, and lead employees to different results in similar situations. Formalizing processes will assist CETC in maturing and allow it to address turnover, capturing information before personnel leave, as occurred in the content management and the request for information shop. One of the only written resources used on a semi-regular basis, the OSCO Cookbook, has never been reviewed by the G4, does not have a formal review process and does not have a means for the workforce to recommend changes. The Cookbook is supposed to be a living document and it needs updating. By creating formal SOPs and SOP processes, this vital reference document can be updated quickly and correctly as the OSINT field grows and changes.

### C. Expand workplace resiliency programs

Workplace resiliency consists of recognizing the challenges and stressors presented by the job; ensuring employees are aware of and encouraged to use available resources, including the Employee Assistance Program, to assess and overcome those stressors; and making efforts to overcome the perceived stigma associated with using such options.

Workplace resiliency is especially important following deployments, particularly to locations in which employees are in close proximity to unpredictable and dangerous situations. Information regarding the full range of EAP services – including everything from assistance securing childcare during a physical absence to counseling services – should be supplied to individuals who deploy. In addition, the operational plan for each deployment should include a post-deployment resilience element. As appropriate, agency or division leadership should reach out to individuals before and after their deployment. Managers should also consider whether public and private recognition through a letter or award is appropriate following a deployment.

Workplace resiliency is also important following negative attention on the agency, particularly if there is uncertainty about whether individuals will face any repercussions for their actions. To be effective, workplace resilience efforts – such as listening sessions, EAP presentations, leadership lectures, and other programs – must be supported by I&A leadership, and employees must be encouraged and given time to participate. I&A leadership should acknowledge that people make mistakes and should emphasize the importance of learning from and moving past mistakes.

Likewise, to be successful, inclusion events, which promote open communication and establish a sense of community, must be attended by senior leadership.

In addition, open meetings, such as town hall meetings, are an effective way to foster communication between I&A leadership and staff. I&A staff should have a forum to ask questions and voice their views without fear of retaliation and with an expectation that fair questions will be answered and consideration will be given to grievances.

### D. Conduct a holistic review of the strategic direction of I&A

The role of I&A's mission centers, the buy-in from SLTT partners and the DHS IE, and the impact I&A has on informing intelligence questions or preventing violence all deserve renewed consideration. Objective evaluation of the reorganization conducted over the past three years could ascertain where gains occurred and where the organization regressed or lost needed capacity.

### E. Resolve when unmasking is appropriate

The IO Guidelines and EO 12333 clearly permit unmasking in certain situations with regard to PII. However, from a policy perspective, a default setting for masking creates an important last guardrail for information improperly collected, retained or disseminated. In a threat situation,

unmasking the subject does make sense. This is an issue that one would expect to be addressed in training and SOPs. However, first an I&A policy is required. That policy should define under what situations USPI should be unmasked and the decision level, at a point sufficient to allow adroit, yet deliberate operations.[487]

As a related but smaller matter, the issue of whether a social media handle is PII appears yet unresolved, and is a point of confusion to collectors. ILD, IO and operators should work out a solution and disseminate it.

### F. Restart the OSIR process

1. Collector Engagement.

The events of the past July and the different investigations have repressed the collectors' efforts. Part of the problem is training, part is adequate SOPs, and part is confidence. The work force needs reinvigoration.

2. Collection plans should exist prior to engaging collection.

Across the IC, standard practice is that before one engages in collection, one first starts with the creation of a collection plan. Collection plans require the collector to identify the intelligence need they are filling, find the EEIs and PIRs that they are collecting to, and the means by which they are going to collect that information. On top of organizing a collector's thoughts into a trackable document, doing so forces the collector to collect to the requirement rather than seeking what they presume is reportable information and attempting to squeeze the information discovered into a collection requirement. Instituting collection planning in OSCO would help build a culture of compliance by making collectors look at requirements, improve tradecraft by having collectors think about their plan before they begin collection, and would provide CETC leadership a new source of data for metrics, research, training, and evaluation of their employees.

### G. Fix the OSIR release process

1. General.

The OSIR release process is broken within CETC. The two SDOs are overwhelmed by the volume of reports and hamstrung by antiquated technology and multiple collateral duties. CETC should consider splitting the content management and supervisory roles, expanding the hiring pool for those positions, and replacing HOST.

2. Split the supervisory and SDO role.

[487] After the Portland incident, CETC issued a policy to its workforce that requires masking of all PII regardless of the topic, and requires any entities desiring masked PII to use the RFI process. This policy does not take into consideration the current authorities that exist to unmask in appropriate circumstances, nor does this policy apply to any I&A section other than CETC. CETC Memorandum, Masking and Dissemination of Open Source Intelligence Reports (OSIR) Containing Personal Identifiable Information (PII) (Sep 14, 2020).

When CETC was a much smaller organization producing far less reporting, the role of content management was held, full time, by two senior employees. The number of supervisors has not changed despite a 200% increase in personnel and an exponential growth in reporting. SDOs cannot focus on publishing OSIRS if administrative duties consume their time. As discussed below, making DOs supervisors might also help solve this problem.

3. Expand the hiring pool for supervisors.

CETC needs to expand the possible hiring pool of SDOs or CRAs to all experienced release authority professionals. Since OSIRs are based on IIRs, which use a standard format for raw reporting used across the IC, there is likely a large pool of qualified professionals who can manage content effectively. Expanding this pool may bring down costs on bringing on new SDOs to review and publish OSIRs.

4. Replace HOST.

HOST was never supposed to be a final product, but rather a proof of concept by an employee. The program only allows one person at any given time and it is plagued with instability issues in part due to Microsoft's dwindling support for the program. Today, no shortage of databasing and distribution software exists that has been fed ramped – purchasing a commercial replacement for HOST could provide a quick, stable solution, that could come with contracted support over the life of the system. Having a more usable and stable distribution tool for SDOs would allow them to work on different issues and greatly reduce the time from the writing of OSIRs to customer consumption.

**H. CETC review**

1. Evaluate whether 24/7 operations are necessary for OSCO, or if *maxiflex* with surge support will suffice.

The move to 24/7 operations at OSCO has created low morale and high turnover, while increasing personnel requirements and resource costs. Is the value of reports produced at night commensurate with the value of resources expended to staff on the night shift?

2. Evaluate the utility of non-FOD deployments.

Many personnel sent to Portland deployed without any real plan for their use or were engaged in activities that could be completed from their normal duty station. However, this does not mean that I&A's presence and activity was not appreciated or provided value to the overall DHS operation. In order to determine the utility of deployments, I&A needs to examine utilization of I&A information and personnel by the other members of the federal response in Portland to ascertain if the marginal value exceeded that of the cost of deployment.

3. Consider returning OSCO reporting back to functional areas rather than general threats.

The shift to threats removed OSCO's former focus on subject matter expertise and portfolios aligned with mission center areas and instead focused on threats. Reporting increased thereby, but the shift also resulted in a decrease in intelligence utility, as measured by OSIR inclusion in finished intelligence products. Following the events surrounding Portland, OSCO has stopped exclusively focusing on threats. CETC needs to determine what is the appropriate balance between portfolio-based collection vis-à-vis tactical threat-based reporting.[488]

Related to the above, the "duty to warn" is not an enumerated mission. Rather it is an obligation when I&A finds a direct threat to a person in the course of intelligence activities. Although certain collection requirements may be more likely to provide a greater quantity of incidental duty to warn obligations, CETC should consider whether the focus on threats occurs to the detriment of other broader missions. Narrowing OSCO's aperture to only threats comes at a huge opportunity cost, while potentially duplicating similar efforts by I&A entities with better relationships and who are less constrained to talk to SLTT and other federal law enforcement.

4. Consider making CETC desk officers (DOs) supervisors.

The DOs in OSCO are non-supervisory team leads. This leaves them in a somewhat awkward position of being a senior person with responsibility to review, help and direct collectors without any authority. Furthermore, without lower level supervisors, the first-line supervisors are the SDOs, who are often overwhelmed or unavailable for certain shifts or certain days. Making the DOs supervisors would enable them to better serve those on their shift and improve OSCO efficiency. Doing so would also create an intermediate leadership development position. If DOs are made supervisors, the appropriate position description should be created through OCHCO.

5. Better integration with ILD.

CETC's relationship with ILD is counterproductive to both offices. Personnel on both sides need to work better together. Communication between ILD and CETC must improve in order to better anticipate potential issues and ensure that problems do not metastasize.

6. Reconsider OSIR quotas.

CETC needs to reconsider the quota system for OSIR production. An emphasis on quantity vice quality encourages collectors to over-report, or try to apply collection requirements that do not fit. Given the other systemic issues in CETC, over-reporting further strains existing systems and processes.

7. Validate an OSIR review process.

The current OSIR review regime is untenable: collector to peer review to DO to OSCO lead to CETC Deputy to CETC chief to the DUSIEO. This is overkill, and cannot support efficient

[488] Apparently, post-Portland, OSCO has shifted back to 80% portfolio-based, 20% threat based search paradigm. Ex. A58. The issue with the change is not the specific breakdown of portfolio -- threat searches -- but the analysis and discussion behind doing so.

release of OSIRs. CETC needs to create a realistic release plan that also accounts for situations requiring greater leadership involvement.

**I. CETC – NOC relationship**

There needs to be a defined relationship and a delineation of mission equities and duties amongst CETC and the NOC. Both provide valuable timely information to a myriad of partners and customers; however, currently both overlap and underlap for different events. The duplication serves neither organization nor the larger goal to keep leadership and partners updated and to provide timely, actionable information. A delineation of duties and a better partnership should be memorialized in writing ascribing actions and responsibilities to maximize the utility and capabilities of both organizations.

**J. Coherent deployment operations require planning.**

1. Create an off-the-shelf Incident Action Plan (IAP) that can be used as a framework for deployments, prior to crises taking place.

Portland's deployment happened abruptly and without adequate planning. Mr. Murphy asked for a new OPLAN for Portland, and people deployed from across different elements including those not initially included in the OPLAN. This led to, among other things, sending people to Portland without any operational need or purpose to their presence. This is a waste of resources. If I&A believes that such deployments may be necessary in the future, I&A should create contingency plans that they can option in a crisis and that are adaptable to the situation. By engaging in this type of planning I&A will at least understand its own capabilities to the point that they know what an office can provide and when a deployment is reasonable.

2. FOD should consider incorporating other I&A elements in its plans.

FOD did have plans for deployments and coordination of I&A activities in a deployment, but those plans and processes were only known to and only included FOD regarding deployment of I&A employees. When other I&A employees arrived in Portland, they ignored the SOP and policy that said that FOD was in command. OSCO refused to coordinate with the FOD lead and organized their own work and schedule. A lack of a unity of command in an operational environment can lead to disjointed activities, wasted effort, and potential mission failure. Formalizing FOD's processes as I&A processes at the I&A level would provide FOD with the necessary legitimacy and authority to represent the whole of I&A in any situation and ensure the other elements of I&A respect and coordinate with the FOD lead during a crisis.

**K. Operational Background Reports (OBRs) review and training.**

1. OBR review.

As is discussed above, two issues exist regarding the OBRs produced during the Portland incident. First, a sufficient reason may not have existed to create certain OBRs in the first place.

Some persons for whom an OBR was produced had "failure to comply" listed as the sole reason for arrest. Others had no reasons listed for arrest. Regarding American citizens, in the context of mass protests or protection of critical infrastructure, production of an OBR requires at least an arrest for a federal crime or more detailed information that the subject poses a considerable threat. Second, OBRs may have been improperly disseminated. If I&A has retained any OBRs from Portland, those OBRs should all be reviewed to ensure that retention is proper, and if dissemination occurred, that dissemination was proper. Our understanding is that the I&A Intelligence Oversight Office is currently examining this issue.

2. Future OBR use.

OBRs can be a valuable tool to produce the background of a person who poses a threat to the homeland or is accused of committing an act that threatens homeland security or law enforcement officers' lives. However, given the apparent misuse of OBRs, some training by the G4 on the proper circumstances to use and disseminate OBRs may be warranted. This training should include leadership given that staff officers recognized the issues presented by creating the OBRs; leaders did not.

3. CETC OBR SOP.

The CETC OBR SOP should be recalled, revised and reviewed to include the proper circumstances for use of an OBR, before re-release. I&A may wish to consider whether the SOP should be reprinted as an I&A directive.

**L. Murphy at I&A.**

As is indicated throughout the Findings, I&A is an organization in need of repair. Some of the identified issues are not the direct fault of Mr. Murphy and actually pre-date his appointment as PDUSIA. Other issues arose and festered as a result of the negative organizational culture and command climate fostered by Mr. Murphy as a preeminent leader of I&A. Finally, this review identified issues for which Mr. Murphy bears direct responsibility during his tenure as PDUSIA and Acting USIA (e.g., unmasking, the VAAI definition). The work climate created by Mr. Murphy not only raises concerns about a potential toxic work environment for his employees, but it led to at least three questionable intelligence activities in three months that were attributable to his refusal to entertain counter opinions and a failure to consider staff input once he decided on a course of action.

In order to address the issues this report covers and to prevent similar issues from occurring in the future, the work climate, fear of retaliation, and marginalization of oversight problems created by Mr. Murphy must continue to be faced head on. Moreover, I&A must continue to have leadership who will restore trust and confidence in its workforce and its partners. I&A must have leadership who has credibility, who will listen, and who is capable of forging consensus. I&A must have leadership who will be able to set clear goals and then obtain buy-in on I&A's plan of action to address the organization's problems. Senior leaders in I&A do not

think Mr. Murphy provides that leadership.[489] And Mr. Murphy himself does not appear ready to provide that leadership. Mr. Murphy did not indicate that he is aware of, let alone concerned with, the criticisms regarding his leadership. Nor does he take responsibility for any missteps under his watch.

Due to the issues he created, fostered, or ignored, and his apparent unwillingness to acknowledge and address these issues, Mr. Murphy is not the right person to make the necessary changes and restore the trust that I&A needs right now. DHS leadership should strongly consider ensuring that Mr. Murphy not return to lead I&A in any capacity.

[489] *See, e.g.,* B49 (Memorandum for Record, subject: Brian Murphy, dated December 8, 2020).